Engineering Science and Technology, an International Journal xxx (xxxx) xxx

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch

Review

A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks

Juan Fernando Balarezo *, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan

RMIT University, 124 La Trobe Street, Melbourne, VIC 3000, Australia

ARTICLE INFO

Article history:
Received 30 March 2021
Revised 29 July 2021
Accepted 23 September 2021
Available online xxxx

Keywords:
Networks security
Attack modelling
Distributed Denial of Service (DDoS)
Software Defined Networks (SDN)
Virtual networks
Traditional networks

ABSTRACT

Denial of Service and Distributed Denial of Service (DoS/DDoS) attacks have been one of the biggest threats against communication networks and applications throughout the years. Modelling DoS/DDoS attacks is necessary to get a better understanding of their behaviour at each step of the attack process, from the Botnet recruitment up to the dynamics of the attack. A deeper understanding of DoS/DDoS attacks would lead to the development of more efficient solutions and countermeasures to mitigate their impact. In this survey, we present a classification approach for existing DoS/DDoS models in different kinds of networks; traditional networks, Software Defined Networks (SDN) and virtual networks. In addition, this article provides a thorough review and comparison of the existing attack models, in particular we explain, analyze and simulate different aspects of three prominent models; congestion window, queuing, and epidemic models (same model used for corona virus spread analysis). Furthermore, we quantify the damage of DoS/DDoS attacks at three different levels; protocol (Transmission Control Protocol-TCP), device's resources (bandwidth, CPU, memory), and network (infection and recovery speed).

Contents

* Corresponding author at: Unit 1514 160 Victoria Street, Carlton, VIC 3053, Australia.
E-mail address: s3738234@student.rmit.edu.au (J.F. Balarezo).

https://doi.org/10.1016/j.jestch.2021.09.011
2215-0986/

Please cite this article as: Juan Fernando Balarezo, S. Wang, Karina Gomez Chavez et al., A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks, Engineering Science and Technology, an International Journal, https://doi.org/10.1016/j.jestch.2021.09.011

1. Introduction

Traditional networks require great effort in order to be deployed and managed [2], because both control and forwarding plane reside within the same physical device. Network administrators must plan very carefully when they are asked to perform any modification in the network, especially in large scale networks. The complexity relies on the fact that any configuration change requires that every associated device is configured accordingly. Leading to the possibility of having several issues like human mistakes, incompatibility between devices, network malfunctions, service outages and so on. Moreover, traditional networks lack of dynamism, due to a complex (sometimes impossible) automatic reaction to failures or workload variations. Software Defined Network (SDN) is an emerging networking technology where the control plane is separated from the forwarding devices (routers and switches) and it is implemented as a centralized controller [3]. This approach makes the network more flexible and easier to be managed by network operators because modifications and new configurations can be performed from a central point. SDN architecture, centralized management and programmability features provide some benefits compared to traditional networks, such as wide visibility and flexibility. However, these features imply that some security issues need to be taken into account, such as Denial of Service (DoS) or Distributed Denial of Service (DDoS).

Over the years, communication networks have faced several challenges. Delivering acceptable levels of security by assuring the three cornerstones of information security, i.e. confidentiality, integrity and availability [4], has been one of the biggest challenges. Within security threats, DoS/DDoS have become one of the most dangerous over the Internet. The ease and cheap ways of performing DDoS attacks have allowed their exponential growth, they have reached magnitudes over 1.7 Tbps in 2018 [5]. Therefore, it is relevant to clearly understand the dynamics of these kinds of attacks to develop efficient mitigation techniques. DDoS attacks within traditional networks can be classified into volumetric attacks, protocol exploitation attacks and application attacks [6]. Meanwhile we classify SDN DDoS attacks according to the affected plane, i.e. data plane, control plane and application plane. More details regarding the different types of attacks will be elaborated later in this paper.

The goal of this survey is to evaluate the existing DoS/DDoS attacks models for traditional, SDN and virtual networks. So far, attack models have been developed for traditional networks such as mathematical models based on traffic engineering [7] and the TCP congestion window [8], analytical models based on probabilities [9,10], hierarchical models based on attack trees [6], semantic models [11] and epidemic models [12]. However in SDN there are only few DDoS attack models developed in the literature [13,14]. A similar situation happened for virtual networks, where only few mathematical attack models were found [15,16]. Therefore, due to the relevance of DDoS attacks nowadays and the lack of attack models for SDN networks, this survey presents:

- We analyze the traditional network DDoS attacks and propose a classification of SDN DDoS attacks represented by an attack tree in order to identify similarities and differences from traditional networks DDoS attacks. SDN DDoS attacks classification allows us to identify the attack vectors that have more impact on SDN. Then we can focus our research on those attacks.
- A comprehensive review of different mathematical models for traditional, SDN and virtual networks. Where we observed a lack of models in the literature compared to the amount of mitigation solutions. Subsequently, to provide optimized mitigation mechanisms a deeper understanding of the attacks is required. This knowledge can be obtained through modelling. Most of the models in literature were developed for traditional networks. Being DDoS attacks a big threat in SDN, it is necessary to adapt or develop models for SDN.
- Additionally, we found that three existing models for traditional networks can be adapted to SDN. The models encompass resources that can be modelled in the SDN architecture. We deeply explain, analyze and simulate these DDoS attacks models i) Congestion Window Model which is modelled based on the DDoS Transmission Control Protocol (TCP) attack, ii) Queuing Model which provides the impact of DDoS attacks on the bandwidth, CPU and memory of network devices, and iii) Epidemic Model which models the propagation and damage of DDoS attacks at network level.

The rest of the article is organized as follows. Section II details the types of DoS/DDoS attacks in different kinds of network architectures (traditional, SDN and virtualized). Section III introduces the classification of the existing models, where three models developed for traditional networks are identified to be relevant to SDN. Section IV presents the analysis and comparison of these models through simulations. Finally, Section V concludes this review.

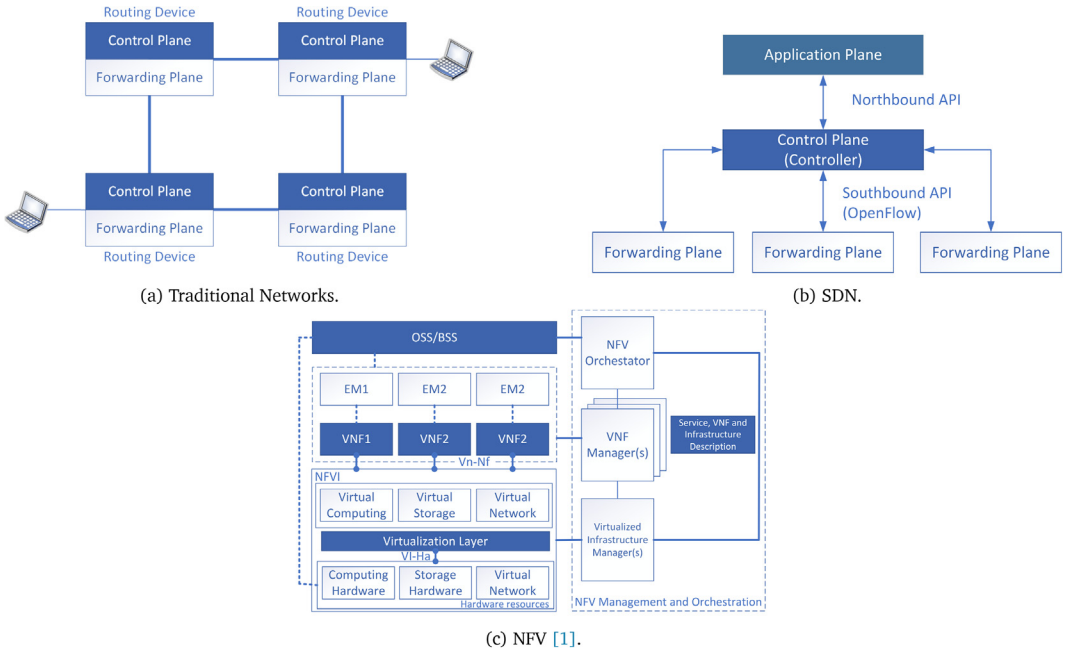
2. Types of DoS/DDoS across networks architectures

Nowadays, DDoS attacks are a growing threat due to the simplicity of execution for these attacks [17]. In this section, we present the classification of DDoS attacks according to the network architecture that is being targeted – Traditional, SDN and Virtual Networks.

2.1. DoS/DDoS attacks in traditional networks

Within traditional networks, control and forwarding functions are performed by each individual routing or switch device [18]. A basic architecture of traditional networks is shown in Fig. 1a, control plane and data plane are embedded in a single networking device therefore distributed control and data plane is the main feature of traditional networks. Historically, these networks have several types of routing devices, where different brands are used, each brand has its own protocols and interfaces, as well as its unique configuration languages. Under this architecture, high-level knowledge and skills are required to implement, manage and troubleshoot such heterogeneous and complex network, which also implies higher costs [19].

DDoS attacks seek to impact the target services or servers quality and even make them unavailable. In order to achieve this goal, different attack vectors can be used to impact traditional networks. Fig. 2 shows the attack tree modelled by [6], with the corresponding attack vectors classified as follows [17]:



(a) Traditional Networks. (b) SDN.

(c) NFV [1].

Fig. 1. Network architecture depicted the control and data plane localization on the traditional, SDN and virtual networks.

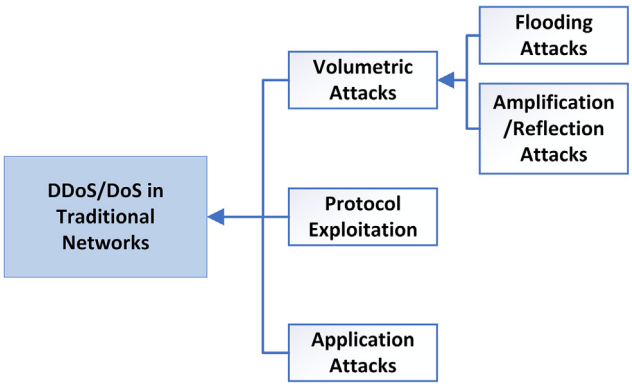


Fig. 2. Schematic classification of DDoS attacks in traditional networks [6].

- **Volumetric Attack:** The target is flooded with traffic in order to deplete the network or hardware resources, the main target is the bandwidth. Within volumetric attacks we can find flooding and amplification/reflection attacks. Flooding attacks seek to exhaust bandwidth, processing capacity or other network resources using large volume of traffic [20]. Meanwhile reflection attacks exploit spoofing vulnerabilities, where the attacker uses forged requests in order to generate traffic from several devices to the victim [21]. Amplification attacks use small requests that generate bigger responses, such as sending several Domain Name System (DNS) requests to a DNS server asking for the complete DNS table, and consequently causing the DNS server to crash.
- **Protocol Exploitation (State Exhaustion Attacks):** This kind of threat seeks to exploit network protocol vulnerabilities and consume the connection state tables that some network devices build [22].
- **Application Layer Attack:** Vulnerabilities are exploited in application layer protocols such as HTTP and SSL. Application code can be vulnerable itself as well when secure-coding practices are not considered. These attacks are the most dangerous since there is no need to generate huge amounts of traffic. Application layer attacks are very difficult to detect because they are stealthy in nature and use legitimate traffic [23].

Attackers can launch several attack vectors at the same time (multi-vector attacks). Multi-vector attacks are used in order to cause greater damage on their targets [24].

2.2. DoS/DDoS attacks in software defined networks

SDN decouples the network architecture into three planes, the control plane, the data plane and the application plane as shown in Fig. 1b. Communication between each plane is carried out through the Northbound and Southbound Application Programming Interfaces (API) [25], which introduces the programmability concept into SDN. This capability allows the configuration and management of the network using open and standard programming languages. Nevertheless, the most commonly used API within the Southbound interface is OpenFlow [26]. OpenFlow protocol is used to establish communication (using TCP) between the control plane (controller) and the data plane (forwarding devices). OpenFlow protocol allows the controller to install network policies in the data plane devices (these policies are named flow entries). Based on these flow entries, the networking devices will then have the capability to forward, drop or modify packets when they match any configured entry. In contrast to traditional networks where traffic is normally handled based either on MAC or IP addresses [18].

In the Northbound interface we can find different types of APIs according to their developed purposes, in contrast with the Southbound interface where the most commonly used API is OpenFlow. In order to establish communication between the control plane and the application plane, controllers are able to support several kinds of APIs. The API selection depends on the software running at the application layer [3]. Applications within this plane are mainly used to deliver a high-level interface for network operators to manage the network. These applications translate the operator commands into the controller's language to be processed and forwarded to the data plane devices. Security applications can be

deployed within this layer, such us firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and DDoS mitigation tools.

It should be noted that the controller is the brain of SDNs, this centralized architecture makes them prone to DDoS attacks, something that is unusual in traditional networks. We propose a DoS/DDoS attacks classification for SDNs, which is depicted using an Attack Tree in Fig. 3. As mentioned before, we classify SDN DDoS attacks according to the affected plane. Some of the approaches used to categorize DDoS attacks in traditional networks are considered in our proposed classification within each plane [6,20–23]:

- **Data Plane Attacks:** The attacks target at hosts, applications and routing devices within the data plane. The data plane can be affected by Volumetric Attacks (Flood and Amplification/Reflection attacks), Resource exhaustion or application layer attacks (are only considered the attacks that target applications operating within the data plane). Here all the traditional network attacks can occur.
- **Control Plane Attacks:** The controller is the entity that manages the network, then the control plane is the perfect target for DDoS attacks. It can be affected by attacks that would try to deplete the controller resources. There are also attacks which would try to exhaust the southbound interface bandwidth, blocking the communication between the data and control plane.
- **Application Plane Attacks:** SDN operators can manage the network through the applications installed at the northbound layer, so it could also be a target of DDoS attacks such as Northbound API exhaustion attacks and Application Layer Attacks (in the context of SDN layers). For the latter ones, only those attacks to the applications residing in this layer are considered in this survey.

2.3. DoS/DDoS attacks in virtual networks

Network virtualization was developed in order to provide flexible sharing of physical computing, storage and networking resources in a virtual environment [27]. Virtualized networks have been developing new features and capabilities in recent years, such as the Network Functions Virtualization (NFV) emerging technology [28]. In non-virtualized environments, network functions are implemented using networking devices which comprise vendor specific software and hardware, whereas NFV introduces a different approach for network service provisioning [29]. Main features of NFV technology can be summarized as follows:

- NFV decouples software from hardware, enables a flexible network function deployment and provides a dynamic operation.
- NFV seeks to perform networking functions through virtual environments instead of using hardware devices with the purpose of reducing hardware costs, optimizing network management and improving operational efficiency.
- NFV conceives the implementation of network functions as software-only objects which are executed over the NFV Infrastructure (NFVI) [30].

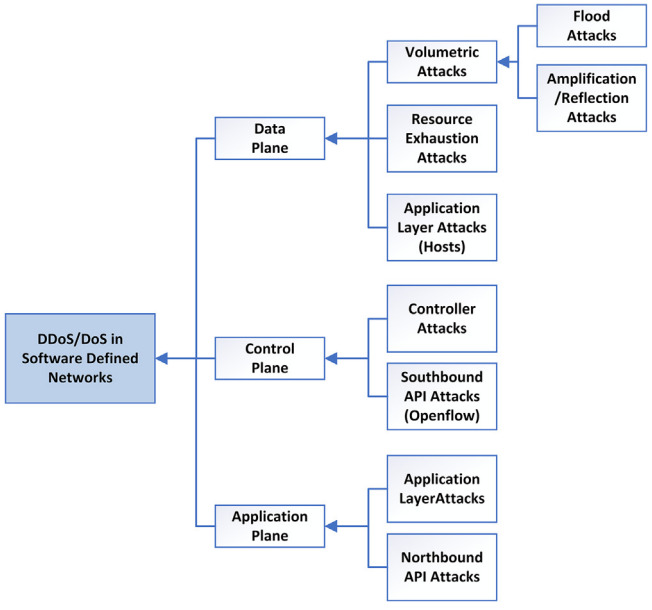


Fig. 3. Schematic classification of DDoS attacks in SDN.

Fig. 1c illustrates the NFV architecture proposed by European Telecommunications Standards Institute (ETSI). NFV comprises three main domains which are: i) Virtualized Network Function (VNF), ii) NFVI, and iii) NFV Management and Orchestration. NFV architecture includes different functional blocks such as VNF, Element Management (EM), NFVI (including hardware, virtualized resources and Virtualization layer), Virtualized Infrastructure Manager, NFV Orchestrator, VNF Manager, Operations and Business Support Systems (OSS/BSS), Service, VNF and Infrastructure Description [1]. These blocks interact between them using reference points.

Similar to SDN, NFV brings changes in networking infrastructure in terms of design, deployment, management [31] and also new challenges come with it, such as security challenges. Virtualization allows to share physical resources (Memory, storage, CPU and network resources) between virtual machines hosted in the same hardware. A DDoS attack targeting the hypervisor or one of the virtual machines, impacts the other ones as well [28]. Then new vulnerabilities can be found due to the existence of the virtual machine manager (VMM) [32]. The same attack vectors that affect traditional networks can target virtualized architectures, but the impact could be even worse since in virtualized environments the resources are shared, for example if a DDoS attack successfully targets the VMM, the whole virtual network could be compromised. Attacks targeting SDN controllers and virtual forwarding devices deployed within a virtual network will also have a considerable impact to the virtual infrastructure. Nevertheless, NFV can help mitigating this kind of attacks due to their dynamic provision, intelligent configuration and optimization detection based software [31]. We propose a DoS/DDoS attacks classification for virtual networks, which is depicted using an Attack Tree in Fig. 4. The attacks are classified according to which component of the virtual architecture is being targeted.

2.3.1. NFV and SDN

The NFV main element is the VMM, or hypervisor, and from this point of view, the VMM provides a service to the network controller (NC) in SDN. Meanwhile from the SDN perspective, the NC is the brain of the system and it provides a service to the VMM [33]. Despite having different frameworks, NFV and SDN complement each other. Then the VMM and the NC have to become components of a single infrastructure resource controller [33]. The Open Networking Foundation (ONF) identifies several areas where SDN and NFV perform similar functions or areas where they can offer services to each other [34]. ETSI also identifies how NFV and SDN should interact [35], a high level view of their proposed integration is presented in Fig. 5. Since NFV and SDN must share common information between each other, they need to agree on shared topics such as security.

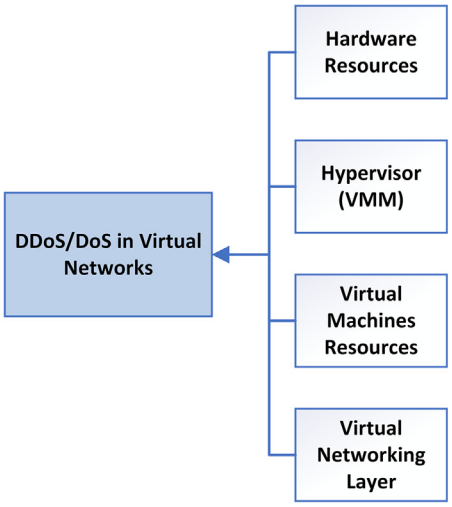


Fig. 4. Schematic classification of DDoS attacks in virtual networks.

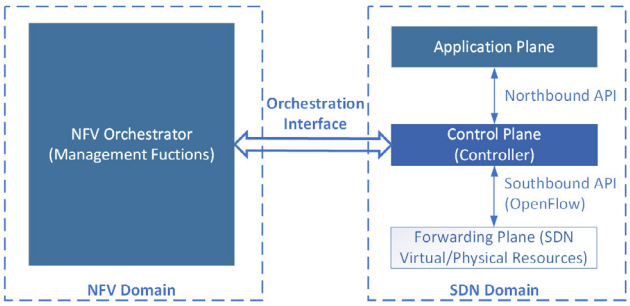


Fig. 5. ETSI NFV-SDN domains interaction [35].

3. DoS/DDoS Attacks Mathematical Modelling

Several detection and mitigation strategies have been modelled and developed to protect assets against DDoS attacks [36–47,23,48], nevertheless there has been limited work on attack modelling. *Attack modelling is essential to understand any threat in depth and to evaluate the associated success factors [10], as well as it can help to evaluate the effectiveness of defense mechanisms [9].* Therefore, attack modelling becomes indispensable to improve the existing mitigation solutions, as found in the existing literature where some models also propose detection and mitigation mechanisms. Additionally, attack modelling can be useful in simulation and emulation of networks as well as for testing the robustness of the network in the design phase. In this paper, the attack models are classified according to which type of network they are designed for, either traditional, SDN or virtual networks. Most of the available models have been designed for traditional networks, but it is possible to apply some of their basic concepts to SDN architecture as well. Once the type of network is identified, the modelling technique used is analyzed for classification purposes, as well as if the model also includes a mitigation strategy or not. The classification flow chart is shown in Fig. 7. In the following subsections, we summarize the attack models according to the classification proposed in Fig. 6, with an overview of the models presented in Table 1. Also a comparison between the models within the same classification is presented in Tables 2–6, where the advantages, gaps and used parameters are analysed.

3.1. DoS/DDoS attacks modelling in traditional networks

Different attack models have been proposed in the literature, however only few of them have used meticulous mathematical models to analyze DDoS attacks [52].We present the existing models in literature for traditional networks based on the approach used when they were developed.

3.1.1. Traffic based models

Traffic based models take into account the behaviour of the attack patterns as well as the network environment [8]. Ramanauskaitė et al. [7] proposed a model as a multidimensional problem, where three different resources -bandwidth, memory and CPU- are the attack targets simultaneously. The model was developed using queuing theory which allowed the authors to get the estimation of the different types of DDoS attacks. In a similar way [53] used queuing theory, nonetheless their system only took into consideration one affected resource. Luo et al. [8] presented a model to calculate the attack effect of low-rate shrew DDoS analyzing the behaviour of the TCP congestion window. Shrew attacks exploit vulnerabilities in the retransmission timeout mechanism used in TCP. As result of their research they proposed a formula to calculate the minimum cost to launch a successful attack and the maximum effect of a shrew attack. Alaoui et al. [49] also considered the TCP protocol behaviour under DDoS attack, they proposed a secure Active Queue Management (AQM) mechanism to stabilize the routers queuing process. The TCP/AQM system was modelled for different attack rates, thus the devices performance is degraded. Considering different attack rates results in a closed-loop Markovian Jump Linear System (MJLS). Q. Huang et al. [51] modelled DDoS attacks that target 3G wireless networks in order to identify

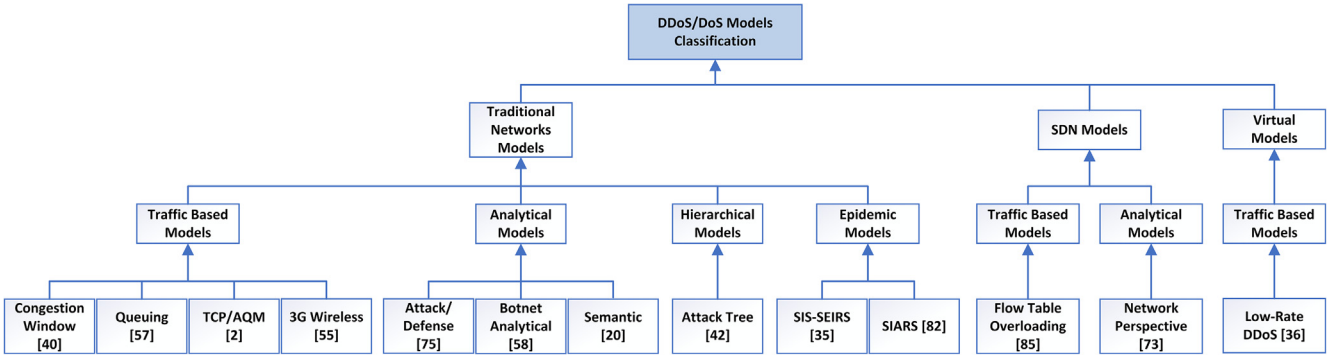


Fig. 6. DDoS models classification based on the works in the literature for traditional, SDN and virtual networks.

Table 1
Summary of the DDoS attack mathematical models available in the Literature.

Model Type	Description	Main Findings
Congestion Window Model [8]	On a Mathematical Model for Low-Rate Shrew DDoS.	The combined impact of attack pattern and network environment on attack effect is evaluated by capturing the adjustment behaviors of victim TCP congestion window. It is found out how to adaptively tune the attack parameters to improve its attack effect in a given network environment, and how to reconfigure the network resource to mitigate the shrew DDoS with a given attack pattern.
Queuing Model [7]	Modelling of Two-tier DDoS by Combining Different Type of DDoS Models.	Two-tier model is more precise for smaller scale attacks, big scale attacks are more concentrated on one resource exhaustion. DDoS attacks target different type of victim resources and should be modelled as composite system.
Attack/Defense Analytical Model [9]	An Analytical Model for DDoS Attacks and Defense.	A real application of the model is proposed which allows to estimate an optimal investment on security.
Botnet Analytical Model [10]	Modelling influence of Botnet features on effectiveness of DDoS attacks.	The proposed attack model could be used for analyzing probability of victim resistance to DDoS attack. Modelling results with different botnet agent allocation strategies have shown the dependence of DDoS success probability on attack power dynamics.
Semantic Model [11]	The modelling and comparison of wireless network denial of service attacks.	The model checker is able to find previously known semantic DoS attacks against 802.11. A new deadlock vulnerability was found in 802.11i which was experimentally validated, facilitating the design of robust protocols by discovering vulnerabilities during the design process.
Hierarchical Model [6]	Impact of a DDoS Attack on Computer Systems: An Approach Based on an Attack Tree Model	The attack tree indicators show the impact of several threats and simultaneous attacks which maximize the system downtime (multivariate analysis).
SIS-SEIRS Epidemic Model [12]	Dynamic Model on DDoS Attack in Computer Network.	An epidemic framework is provided, which consists of two sub frameworks, each one representing the internal and external class of nodes.
Network Model [13]	SDSNM: A Software-Defined Security Networking Mechanism to Defend against DDoS Attacks.	Security mechanism proposed. Approach can be implemented within a hybrid network and works with Cloud computing technologies.
Flow Table Overloading Model [14]	Defending Against Flow Table Overloading Attack in Software-Defined Networks.	Critical vulnerability found in the size of the flow table in SDN switches. A QoS-aware mitigation strategy is proposed. A practical mathematical model is presented for the studied system.
TCP/AQM Model [49]	Modelling, analysis and design of active queue management to mitigate the effect of DoS attack in wired/wireless network.	TCP/Active Queue Management (AQM) system modelled under different attack rates, resulting in a closed-loop system which is presented as a Markovian Jump Linear System (MJLS).
SIARS Epidemic Model [50]	Understanding Botnet: From Mathematical Modelling to Integrated Detection and Mitigation Framework.	A mathematical model is proposed to represent the involved factors in botnet epidemiology. A detection and mitigation strategy is suggested.
3G Wireless Model [51]	Modelling of Distributed Denial of Service Attacks in Wireless Networks.	Three kinds of DDoS attacks targeting 3G wireless networks are modelled: connection depletion, bandwidth depletion and attacks to ad hoc networks.
Low-Rate DDoS Model [16]	Exploring New Opportunities to Defeat Low-Rate DDoS Attack in Container-Based Cloud Environment.	Low-rate DDoS attack targeting container-based cloud environments is modelled using queuing theory. A mitigation strategy is presented based on dynamic resource allocation.

which resources are vulnerable to different kind of attacks. Connection and bandwidth depletion attacks are assessed, while the feasible types of DDoS attacks in mobile ad hoc networks is also evaluated. Strategies are presented to estimate the required resources to be allocated to provide high performance under attack. The proposed models were designed for 3G Networks and may not be applicable to new generation networks such as SDN or 5G networks.

3.1.2. Analytical models

This kind of models seek out the attack success probability according to specific conditions and parameters. Y. Xiang and Z. Li [9] described a model about the interaction between the attack and defense party, which will determine the effectiveness of the defense system and estimate the optimal security investment. Ramanauskaitė et al. [10] presented a model that makes it possible to calculate the attack success probability based on the botnet size and agent allocation strategies. The model can be used to evaluate the victim resistance probability in different attack and defense scenarios. M. Eian and S. Mjølsnes [11] proposed a semantic DDoS attack model against wireless network protocols which can be used to find protocol vulnerabilities. As a result, the model helps in the design and optimization of protocols during the design process.

3.1.3. Hierarchical models

Availability of systems consisting of several components that can be affected by an attack should be modelled using a hierarchical approach. R. Maciel et al. [6] introduced a hierarchical model based on an attack tree analysis which assesses the effects of DDoS attacks by estimating parameters such as the feasibility, likelihood of an attack, attacker benefits, etc. The attack tree allows the evaluation of the impact of simultaneous attacks to the system.

3.1.4. Epidemic models

Epidemic models can be considered a particular class of analytical models. However, we analyze them in a separate subsection due to the implications that the amount of infected devices (bots) have during DDoS attacks. Bots are machines infected by malicious software that can be used to generate the DDoS attack traffic [54], where a group of bots is considered a botnet. Botnets are an essential element to achieve successful DDoS attacks and their dissemination have to be considered in the modelling process of the whole DDoS attack scenario. Thus, the mathematical abstraction of botnet propagation needs to be studied independently. Disease propagation models such as SIS (Susceptible – Infected – Susceptible) and SEIRS (Susceptible – Exposed – Infected – Recovered – Susceptible) [55] can be used to analyze the botnet creation and propagation process. U. Kumar and S. Kumar [12] represented an SIS-SEIRS

Table 2
DDoS attack models comparison for traditional networks - Traffic Based Models.

Model	Model or Solution	Advantages	Gaps	Parameters
Queuing Model [7]	Model	Two-tier attack modelled using query modelling (Multidimensional approach)	No dependency between Memory and CPU during attack is considered. The model can only be applied for one channel (K = 1).	Attack Success Probability, Bandwidth Exhaustion Model, Memory Exhaustion Model, CPU Exhaustion Model.
Congestion Window Model [8]	Both	Provides some novel properties of the shrew attack, such as the minimum cost formula to launch a successful attack, and the maximum effect formula of a shrew attack.	The defense mechanism does not work with high rate data streams. The model assumes that the TCP sender's window size is not affected by the receiver's advertised flow control window.	Bottleneck buffer size and bandwidth, One-way propagation delay, Acknowledged packets, Attack period, Attack peak length, Peak magnitude, Attack effect, TCP sender's congestion window.
TCP/AQM Model [49]	Both	Model based in a time-driven TCP/ AQM system under DDoS attack, allowing the analysis of secure AQM mechanisms to stabilize queuing behaviour.	Model needs to be extended to a discrete time domain. The model only uses a known transition matrix, partially unknown and unknown matrix should be also studied.	Average congestion window size, Round Trip Time, Dropping packets probability, Queue length, Link capacity, Propagation delay, Window distribution parameter.
3G Wireless Model [51]	Model	Three different models are proposed to represent different types of DDoS attacks targeting 3G wireless networks.	The models are developed for the 3G legacy network. No mitigation technique is provided, only a prevention strategy.	Connection requests, Arrival rate, Holding time, Service time, Connection loss probability, Link capacity, Buffer capacity, Number of agents.

Table 3
DDoS attack models comparison for traditional networks - Analytical and Hierarchical Models.

Model	Model or Solution	Advantages	Gaps	Parameters
Botnet Analytical Model [10]	Model	Provides influence estimation of Botnet size and agent allocation strategies on attack success probability.	Assumes constant legitimate traffic rate only.	Attack Prevention Probability, Attack Mitigation Probability, Attack Postvention Probability.
Hierarchical Model [6]	Model	Provides the equations that estimate the likelihood of an attack, attacker benefits, feasibility, the pain factor and the propensity of the offense.	It is a hierarchical based approach which indicates the likelihood and impact of the attack, there is no attack model based on traffic.	Successful attack probability, Occurrence likelihood, Cost of attack, Attackers benefits, Feasibility, Noticeability, Technical ability, Pain factor, Operational losses.
Attack/ Defense Analytical Model [9]	Model	An analytical model for the interactions between DDoS attack party and defense party is proposed, which can be used to estimate the effectiveness of a DDoS defense system.	It is an analytical based approach, there is no attack model based on traffic and some factors from each party are not considered.	Attack/Defense parties, Attack/ Defense strength functions, Time, Mitigation rate, Attack rate, Security investment, Defense Budget, Vulnerability, Potential loss.
Semantic Model [11]	Model	The model allows to evaluate the efficiency of DDoS attacks that target wireless networks and to discover protocol vulnerabilities.	The adversary model does not include all parameters, while the cost model could be improved to deliver more realistic results. Experimental test is briefly explained, more details are needed.	Party protocol, Initiator, Responder, Protocol cost, Adversary cost, Initiator cost, Responder cost, Attack efficiency.

model to evaluate the propagation of bots in communication networks in order to understand the dynamism of the model members. As a result, an epidemic framework is obtained which consists of two sub-frameworks represented by the external and internal network, but they are treated as a single universe when they need to be analysed independently. W. Yong et al. [50] proposed a mathematical model that analyzes the factors involved during the botnet proliferation process, modifying the SIRS model into a SIARS model, where the Active state is introduced. Based on the proposed model, W. Yong et al. [50] presented a detection and mitigation framework. The presented model limitation relies in the fact that internal and external networks and hosts are not appropriately segregated. V. Matta et al. [56] presented a threat propagation model using the Birth–Death-Immigration (BDI) approach. In first place, their model assumes that the attack parameters are known in order to optimize the resource allocation process. Then, they remove the assumption about the attack parameters in order to estimate them with maximum-likelihood estimators. The model does not specify if the nodes get permanent immunity or not, which clearly needs to be addressed since new vulnerabilities can be found within the cured nodes. M. Gardner et al. [57] described the spread of IoT worms using the IoT Botnet with Attack Information (IoT-BAI) perspective, which follows a variation of the SEIRS epidemic model. The authors proposed that improving user information will positively affect the user behavior. Thus, reducing substantially the potential for successful DDoS attacks. However, the ways that the user behaviour can be improved and the type of information that needs to be provided is not detailed.

Table 4
DDoS attack models comparison for traditional networks - Epidemic Models.

Model	Model or Solution	Advantages	Gaps	Parameters
SIS-SEIRS Epidemic Model [12]	Model	An epidemic SIS-SEIRS model is proposed to represent the propagation of bots. Also the dynamism of the members of different sections of the model is represented.	The model does not specify the impact of the DDoS attack to the computer system as well as the variable allocation method is not specified.	Susceptible, Exposed, Infectious and Recovered nodes, Transition rates, Recovery rate, Birth rate, Reproduction ratio, DDoS death rate.
SIARS Epidemic Model [50]	Both	The model estimates the reproduction number, allowing to predict if the epidemic will proliferate or not. Active state added to understand the real outbreak scenario.	The model does not segregate the behaviour of the internal and external nodes during the process.	Susceptible, Infectious, Active and Recovered nodes, Transition rates, Reproduction ratio, DDoS death rate.

Table 5
DDoS attack models comparison for SDN networks.

Model	Model or Solution	Advantages	Gaps	Parameters
Network Model [13]	Both	Necessary conditions of DDoS attacks modelled from network architecture perspective.	No mathematical model proposed	Network, Set of hosts, Set of switches, Set of links, Routing Mechanism, Set of target hosts, Set of dummy hosts, Attacker, Attack rate, Attack time.
Flow Table Overloading Model [14]	Both	SDN mathematical model which uses queuing theory to evaluate the DDoS attack impact in the SDN devices' flow table.	Does not consider how other SDN elements are impacted during the attack. The model can be improved in several ways.	Number of switches, Flow table size, Arrival rate, Service rate, Attack rate, Attack duration, Holding time.

Table 6
DDoS attack models comparison for virtual networks.

Model	Model or Solution	Advantages	Gaps	Parameters
Low-Rate DDoS Model [16]	Both	Mathematical model based on queuing theory for container-based (virtual) cloud environments. Dynamic resource allocation strategy is presented for mitigation purposes.	Only focused on low-rate DDoS attacks and not considered other cloud oriented attacks. Container treated as a single thread device when it can run multi-thread services as well.	Available resources, Number of containers, Service rates, Arrival rates, Staying times, Malicious users, Malicious requests.

3.2. DoS/DDoS attacks modelling in software defined networks

Only few SDN attack models have been proposed since these kind of networks are still at their early ages of development compared to traditional networks. X. Wang et al. [13] modelled a DDoS attack in SDN from a network architecture perspective and the required conditions for a successful attack. The model is a network representation, and it is not considered as a mathematical model itself. However, the authors presented a security mechanism to mitigate DDoS attacks using strict access control policies. B. Yuan et al. [14] proposed the flow table overloading attack model using queuing theory, which highlights the flow table resource limitation in OpenFlow forwarding devices. The model provides an estimate of the capacity of SDN devices in defending against such attacks. However, the model does not consider how the rest of the SDN elements (such as the controller or the Southbound communication channel) are affected during the attack. A model that contemplates how each component within the SDN architecture is affected by a DoS/DDoS attack is required to have a better understanding of the attack dynamics, as the model proposed by Ramanauskaitė et al. [7] for traditional networks. The lack of proper mathematical DDoS attack models for SDN makes it essential to further research this field because of the impact that these attacks represent to the SDN centralized architecture.

3.3. DoS/DDoS attacks modelling in virtual networks

Traditional and SDN networks can be deployed within virtual infrastructure. Therefore, as mentioned in section II, DDoS attacks vectors targeting traditional and SDN networks can have a critical impact to virtual networks. Z. Li et al. [16] proposed a mathematical model based on queuing theory (traffic based model) to scrutinize how container-based cloud environments behave under low-rate DDoS attacks. Container technology is a lightweight and more flexible way to handle virtualization [16]. Based on the model, they presented a mitigation strategy that handles containers and resources allocation according to the magnitude of the attack.

3.4. Detection and mitigation models

The previous models analyze malicious agents and attack traffic comportment, providing a deep analysis of the attack dynamics and evaluating the associated success factors. Nevertheless, some models in the literature study DDoS attacks from the detection and mitigation perspective. Assessing DDoS attacks directly with mitigation solutions without a previously defined attack model leaves behind important considerations. Also, the focus of our research is attack mathematical modelling, and the detection and

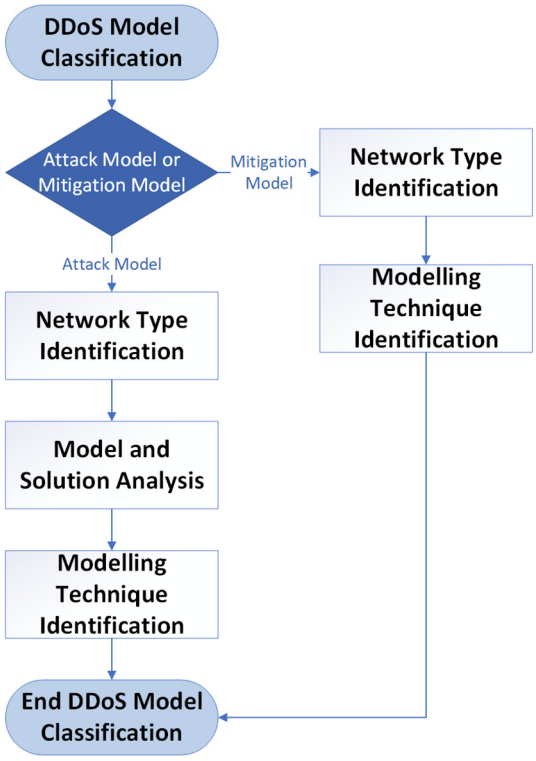


Fig. 7. Model classification process.

mitigation approaches are not part of the scope of our survey, such knowledge can be found in [17,20,46,23]. However, it is worth to contemplate those detection and mitigation techniques that provide insights in attack modelling into our study [58]. Consequently, the detection and mitigation approaches that are relevant to attack modelling are presented below.

- **Traditional Networks:** S. M. Tabatabaie et al. [37] detection algorithm extracts traffic features to build and normalize the packet rate time series. Then the ARIMA model estimates the number of packets in a period of time to analyze the chaotic and non-chaotic errors using the maximum Lyapunov exponent, as it was similarly done in [59]. Another chaos theory based strategy is proposed in [60], where a neural network detection system is implemented. N. Jeyanthi et al. [61] used the Recurrence Quantification Analysis (RQA) mathematical model to detect DDoS attacks. RQA calculates the entropy and determinism from packets' features in order to detect malicious traffic. [62,63] also proposed entropy based models, which are more reliable methods that seek to understand the attack traffic first, rather than simply setting thresholds to drop packets. R. F. Fouladi et al. [64] considered both, sparse coding and frequency domain models, to present an anomaly-based DDoS detection approach, as well as [65–73] presented behaviour based detection mechanisms. E. Vilaça et al. [74] also proposed an anomaly detection mechanism using a machine learning model that applied Robust Principal Component Analysis (RPCA) and Mahalanobis Distance. Different deep learning and machine learning methods, such as reinforced learning, are useful when modelling mitigation and detection techniques [75–79] in diverse scenarios, like analyzing intelligent DDoS attacks patterns. As part of the mitigation process, it is also important to understand where the attack traffic comes from, which is also essential when modelling the attack behaviour. Therefore, botnet detection strategies like cluster expurgation or union rule proposed in [80] become the first step for such task. Then, we need to gather information about the paths that the DDoS traffic traveled through, the amount of traffic that traveled along each path and the network prefixes associated to such traffic. This knowledge will allow to have more informed and effective DDoS defense systems as presented in [81].
- **SDN Networks:** A. Sangodoyin et al. [82] developed a mitigation mechanism against spoofing and flooding DDoS attacks in SDN from the execution of attack simulations using Mininet emulator. The authors propose an architecture based model which represents the emulated network topology. R. Wang et al. [83] used the packet number counter stored in the OpenFlow table in order to calculate the switches flow statistics. Then an entropy model and algorithm are proposed to detect flooding attacks on the edge switches. Some authors [39,84–86] based their detection and mitigation techniques on network traffic analysis in order to identify specific patterns in different types of DDoS attacks. As in traditional networks, machine learning models showed great efficiency when detecting and mitigating DDoS attacks in SDN [87,88]. As the one proposed in K. S. Sahoo et al. [89], in which Support Vector Machine (SVM) is used as the prime attack classifier, in combination with kernel principal component analysis (KPCA) with genetic algorithm (GA). Allowing to select the relevant features and accurate classifiers for attack detection. However, the proposed detection and mitigation approaches lack of a previously defined mathematical attack model.
- **Virtual Networks:** A. Girma et al. [90] presented a hybrid mitigation strategy using entropy and co-variance matrices to detect DDoS attacks in cloud computing environments at network and host levels. S. Yu et al. [91] analyzed dynamic resource allocation in cloud during DDoS attacks. A mathematical model estimates the resource demands using queuing theory. SDN and virtual hybrid environments are taken into consideration due to the flexibility and reliability both technologies can deliver. Therefore, T. V. Phan and M. Park [92] proposed a hybrid machine learning model and an enhanced history-based IP filtering system as DDoS defense strategy for SDN-based cloud environments. As mentioned in Section II, virtual networks and SDN share similar capabilities and often they are deployed together. Consequently, R. Biswas et al. [93] proposed a framework to detect internal DDoS attacks in a datacenter using virtual machines (VMs) in order to monitor internal flows coming from SDN switches. The detection technique is based on flow grouping that analyzes behavioral similarity among the VMs.

4. Analysis and comparison of the DDoS/DoS mathematical models

In the previous section the DDoS attack models are classified according to what type of network they were developed for, and most of them belong to traditional network architectures. Also as shown in Tables 2–6, most of the models deliver the success probability of an attack as final result as shown in the simulations performed by the authors. It was identified that three models from traditional networks are relevant to SDN and can be applied to the SDN architecture. These models include the Congestion Window Model [8], Queuing Model [7], and the Epidemic Model [12].

4.1. Congestion window model: Protocol attack

The Congestion Window Model is selected because it models the DDoS attack, which targets a single network device (server) using an specific protocol (TCP). Therefore, it could be adapted to

the SDN centralized architecture because the communication channel between the controller and the forwarding devices uses TCP (OpenFlow). The Congestion Window Model is developed for low-rate shrew DDoS attacks and analyzes the behavior of the TCP congestion window, taking into account both i) the attack pattern, and ii) the network environment, however the model assumes that the TCP sender's window size is not affected by the receiver's advertised flow control window (rwnd) [8]. The Congestion Window Model is represented as a dynamic system in Fig. 8.

This model provides the effect of the shrew DDoS attack represented as P_w, which is the normalized legitimate throughput probability, and with a lower P_w corresponding to a better attack effect. P_w is expressed by the following equation [8]:

$$P_w = \lim_{t\to\infty} \frac{X_t}{t \cdot C} = \frac{X_T}{T \cdot C} \tag{1}$$

where, T is the attack period, X_T is the number of the legitimate packets successfully sent within T and depends on the bottleneck buffer size B, and C is the bottleneck bandwidth which denotes the ideal burst magnitude that the attack should have to be successful. Therefore, the successful attack probability is *Pwa* expressed as:

$$P_{wa} = \overline{P_w} \tag{2}$$

Simulations are carried out in order to evaluate the model, firstly we considered B variable and a fixed C and secondly we considered a fixed B and C variable. The results of the simulations are shown in Fig. 9, where we can see that the successful attack probability increases when the attack burst magnitude increases and also the successful attack probability decreases while the bottleneck buffer size increases.

4.2. Queuing model: Resources attack

The Queuing Model is selected because it models the DDoS attack when it is targeting the resources of a single network device (router or server) for attacking the network. Thus, due to the centralized architecture of SDN, this model can be adapted as a DDoS attack to the controller, targeting the channel bandwidth, memory and CPU queues associated to it. The queuing mathematical model is represented as a dynamic system in Fig. 10.

The Queuing Model uses a multidimensional approach to analyze how traffic is processed by networking elements, it is based on traffic theory, where the probabilities of Bandwidth (P_B), Memory (P_M) and CPU (P_C) exhaustion are calculated.

- **The Bandwidth Exhaustion Probability** (P_B) is represented as a queuing system M/G/K/K given by the following equation [7]:

$$P_B = \frac{\frac{\rho^K}{K!}}{\sum_{j=0}^{K} \frac{\rho^j}{j!}},\ \rho = \frac{\lambda_B}{\mu_B} \tag{3}$$

  where, K is the number of communication channels and K channels can be used at the same time, however the formula is only correct for $K = 1$, λ_B is the arrival speed, which also defines the DDoS attack strength and μ_B is the service rate of the system.
- **The Memory Exhaustion Probability** (P_M) is represented as a queuing system M/M/N/N given by the following equation [7]:

$$P_M = \frac{\frac{\rho^N}{N!}}{\sum_{j=0}^{N} \frac{\rho^j}{j!}},\ \rho = \lambda_M \cdot t_M \tag{4}$$

  where, N is the amount of session data that can be stored in the memory buffer, t_M is the average service time and λ_M is the arrival speed, which depends on λ_B and P_B as follows:

$$\lambda_M = \frac{\lambda_B \cdot (1 - P_B) \cdot r}{w} \tag{5}$$

  where, w represents the average number of packets in one session and r is the required number of packets to set up the session [7].
- **The CPU Exhaustion Probability** (P_C) is represented as a queuing system M/M/1 given by the following equation [7]:

$$P_C = \begin{cases} 1, & \frac{\lambda_C}{\mu_C} \geqslant 1 \text{ or } L \geqslant t_w; \\ \frac{L}{t_w}, & \frac{\lambda_C}{\mu_C} < 1 \text{ or } L < t_w. \end{cases} \tag{6}$$

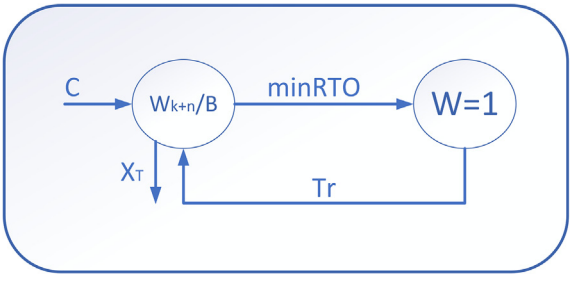


Fig. 8. Representation of the congestion window mathematical model for DDoS attack models.

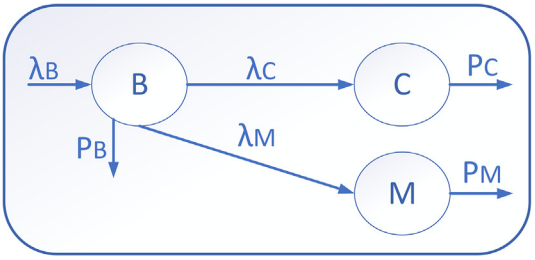
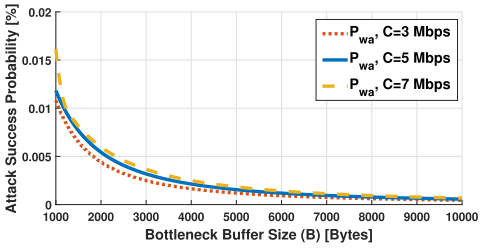
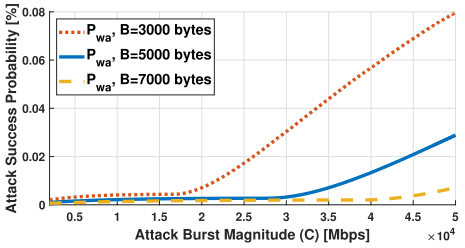


Fig. 10. Representation of the queuing mathematical model.



(a) Bottleneck buffer size (B) variable.



(b) Attack burst magnitude (C) variable.

Fig. 9. Congestion Window Model: Successful attack probabilities (P_{wa}) versus bottleneck buffer size (B), and attack burst magnitude (C) variation.

where, L is the average time a thread spends in the system, t_w is the time the user is willing to wait for a service, μ_C is the service rate and λ_C is the arrival speed, which depends on λ_B and P_B as follows:

$$\lambda_C = \lambda_B \cdot (1 - P_B) + \lambda_S \tag{7}$$

where, λ_S represents the average query arrival speed for service queries [7].

According to [7] the total success probability of a two-tier DDoS attack needs to consider the fact that all the sub-systems involved in the model have an impact between each other. Then, the **Total Probability** (P_q) of successful attack is given by the following equation proposed in [7]:

$$P_q = 1 - \overline{P_B} \cdot \overline{P_M} \cdot \overline{P_C} \tag{8}$$

Simulations are carried out in order to evaluate the model, the used service rate parameters are the same as the ones used in [7], which correspond to $\mu_B = 500\,q/s$, $\mu_M = 100\,q/s$ and $\mu_C = 300\,q/s$. Meanwhile we considered a variable arrival speed, which represents the variation in the magnitude of the DDoS attack. The simulations are done using a one tier model where each attack success probability is independent and also using the two tier model proposed in [7], where the memory and CPU attack exhaustion models depend on the bandwidth exhaustion model. The results of the simulations are shown in Fig. 11, where we can see that the successful attack probabilities increase when the arrival speeds increases.

4.3. Epidemic model: Devices attack

The Epidemic Model is selected because it models how devices can get infected and become part of a botnet, which later could be used to launch DDoS attacks. This model targets several network devices (multiple host, router or server) which later will be attacking the network. Therefore, this model could also be adapted to SDN since the forwarding devices and the controllers themselves can be infected in order to become part of a botnet. The fact that one centralized controller can manage numbers of forwarding devices could lead to a faster propagation process. The Epidemic Model describes an epidemic SIS–SEIRS model in order to illustrate how bots spread in computer networks. Bot infection behaves in a similar way as human epidemics, such as the novel COVID-19 outbreak affects population [94]. The model analyzes the free equilibrium and endemic equilibrium points, determining when they are stable and when unstable. The system representing the epidemic mathematical model is represented in Fig. 12.

In order to determine the stability of the system it is required to find the basic reproduction number of the system. Subsequently, the system has to be analysed when the basic reproduction number is lower than 1, meaning that the infection will not be propagated. And finally analyse when the basic reproduction number is greater than 1. Which is, when the infection spreads but becomes stable at a certain point of time. The epidemic model is represented by the following system equation composed of ordinary differential equations (ODEs) [12]:

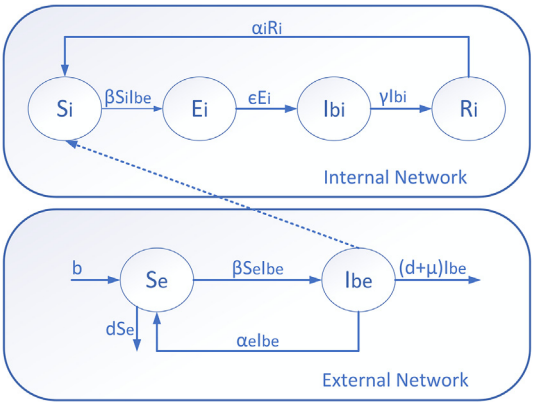
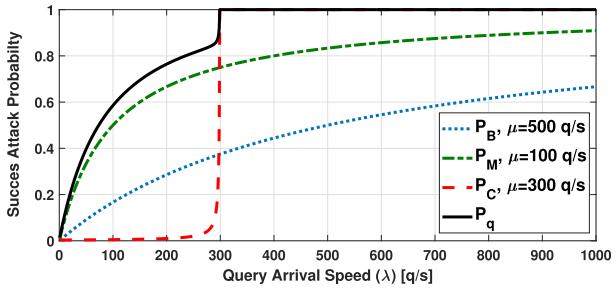


Fig. 12. Representation of the epidemic mathematical model [12].

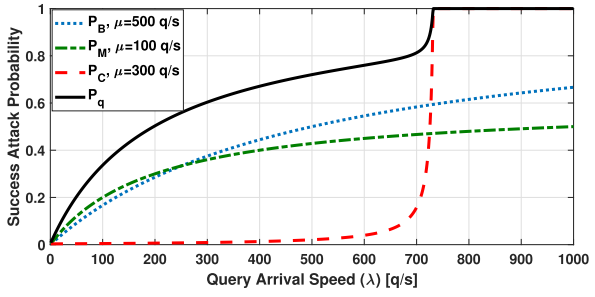
$$\begin{aligned}
\frac{dS_i}{dt} &= -\beta S_i I_{be} + \alpha_i(1 - (S_i + E_i + I_{bi})) \\
\frac{dE_i}{dt} &= \beta S_i I_{be} - \epsilon E_i \\
\frac{dI_{bi}}{dt} &= \epsilon E_i - \gamma I_{bi} \\
\frac{dI_{be}}{dt} &= \beta(1 - I_{be}) I_{be} - \alpha_e I_{be} - (d + \mu) I_{be}
\end{aligned} \tag{9}$$

where,

- S_i and S_e are the susceptible class nodes of total population,
- E_i are the exposed class nodes of total population,
- I_{bi} and I_{be} are the infectious class nodes,
- R_i are the recovered class nodes,
- β is transition rate of the nodes from susceptible class to exposed class in internal network and susceptible class to infectious class in external network. It is important to note that β is considered the same for all equations,
- ϵ is the transition rate of nodes from exposed class to infectious class in internal network,
- γ is the recovery rate in internal network,
- α_i is the transition rate of nodes from recovered class to susceptible class in the internal network due loss of immunity,
- b is the birth rate of the susceptible nodes in external network,
- d is the natural death rate of susceptible nodes and infectious nodes in external network,
- μ is the death rate of infectious nodes in external network due to DDoS attack,

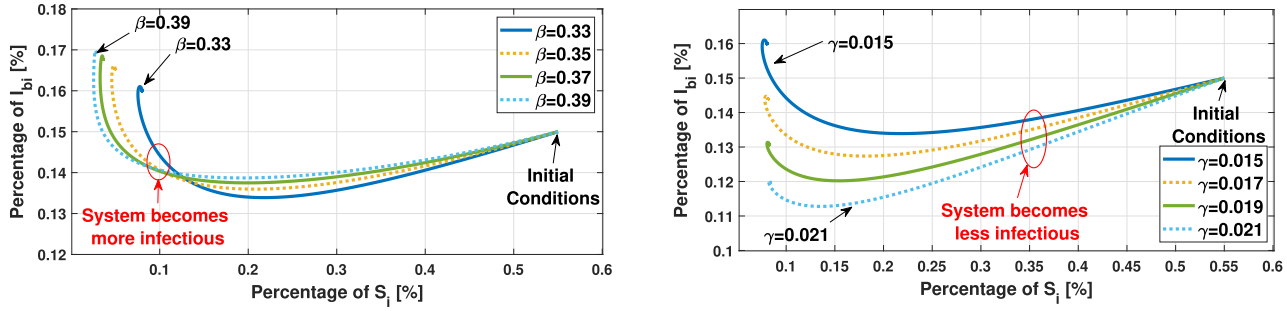


(a) One Tier Model.



(b) Two Tier Model.

Fig. 11. Queuing Model: Successful attack probabilities of Bandwidth (P_B), Memory (P_M), CPU (P_C) and Total exhaustion (P_q) versus query arrival speed (λ) for different service rate (μ).



(a) Percentage of I_{bi} vs. S_i with $\gamma = 0.15$ and β variable.

(b) Percentage of I_{bi} vs. S_i with $\beta = 0.33$ and γ variable.

Fig. 13. Epidemic Model: Susceptible compartment behaviour versus Infectious compartment behaviour for different β and γ transition rates. The initial conditions are: $\{S_i, E_i, I_{bi}, I_{be}\} = \{0.55, 0.15, 0.15, 0.15\}$.

- α_e is the rate of updated run of anti-virus software which transfer the nodes from infectious class of external network to its susceptible class.

Simulations are carried out in order to evaluate the model, the initial conditions used for the simulations are the same as the ones used in [12], which correspond to $\{S_i, E_i, I_{bi}, I_{be}\} = \{0.55, 0.15, 0.15, 0.15\}$. Two kinds of simulations are performed, the first considers eight different values for β and the second one uses eight different values of γ, while using the same values of $\epsilon = 0.004, \alpha_i = 0.015, d = 0.1, \mu = 0.1$ and $\alpha_e = 0.1$ for all the simulations, satisfying the condition that the basic reproduction number is greater than one ($R_{0e} > 1$). Where R_{0e} is given by:

$$R_{0e} = \frac{\beta}{\alpha_e + d + \mu} \tag{10}$$

In Fig. 13a the infectious class nodes (I_{bi}) versus the susceptible class nodes (S_i) of internal network with $\gamma = 0.015$ and β variable are plot. It is possible to visualize that with higher transition rates of the nodes from susceptible class to exposed class in internal network (β) the system becomes more infectious as re-marked on the figure. Instead in Fig. 13b the infectious class nodes (I_{bi}) versus the susceptible class nodes (S_i) of internal network with $\beta = 0.33$ and γ variable are plot. As observed with a higher recovery rate (γ) in internal network the system becomes less infectious as marked in the figure.

4.4. Comparative framework

The three analyzed models consider different parameters to represent the behaviour of DDoS attacks. However, some of the used parameters can be compared within a similar framework, since the models study how the success attack probability is affected by the variation of these parameters. The congestion window model defines that the success attack probability is mainly impacted by the burst attack magnitude and the bottleneck buffer size, which can be said is the system capacity to resist a DDoS attack. Meanwhile, the queuing model proposes that the arrival speed used in queuing theory represents the attack magnitude for the three exhaustion sub-models (Bandwidth, Memory and CPU), while their service rate represents the system capacity to resist the attack. Finally, the epidemic model proposes that a higher amount of infected hosts means a higher probability of a successful attack, since more DDoS traffic can be generated during an attack. Therefore, epidemic models allow to quantify the impact of DDoS attacks because the attack effectiveness can be also measured in terms of the infectious transmission rate [80]. The epidemic model does not mention the system resistance against an attack directly. However, it can be said that reducing the infection rate and having a better recovery rate will reduce the probability of success of the attack.

Finally, Table 7 summarizes the model analysis. These models use different parameters and units, which does not allow to

Table 7
Summarizing the model analysis.

Model	Level	Parameters [Units]	Output	Application
Congestion Window Model [8]	Protocol Attack	Bottleneck Buffer [Bytes], Attack burst magnitude [Mbps].	Shrew DDoS attack effect (Normalized legitimate throughput probability).	Allows to optimize the design of the TCP protocol by tuning the window size parameter and also helps in the design of the server resources.
Queuing Model [7]	Device Resources Attack	Arrival speed [Queries per second], Service rates [Queries per second].	Traffic blockage probability.	Allows a better network design while choosing the appropriate device resources in terms of hardware and software. At the same time it provides an insight of the impact that the attack has at a device level.
Epidemic Model [12]	Network Attack	Susceptible and Recovered nodes [Percentage of devices within the network], Exposed and Infected nodes [Percentage of devices within the network], Transition rates [Number of devices per unit of time].	Percentage of devices within an specific state.	Allows to develop security plans to prevent the spread of infections within the network (anti-virus or detection/mitigation algorithms). It also helps to understand the possible damage that external infections can cause to the internal network.

allocate them within the same exact framework or use the same parameters. Nevertheless, as explained the models rely their success factors in the intensity of the attack versus the available target resources that help it to resist the attack. Based on these parameters they determine the probability that the attacks will be successful or not.

5. Final discussion and conclusions

In this paper we present an analysis about the existing DoS/DDoS attacks mathematical models, firstly categorizing the types of attacks according to which kind of network they target, either traditional, SDN or virtual networks. We found that the amount of mathematical models in the literature is much less compared to the amount of proposed mitigation solutions. Attack models can provide a deeper understanding of DoS/DDoS attacks that would lead us to develop more efficient solutions and countermeasures to mitigate their impact. We classified the attack models we found in the literature according to the type of network they were developed for, the parameters they considered and the way the authors analyzed the network environment and the attack patterns. Most of the attack models are developed for traditional networks, which makes it important to adapt or develop models to the novel SDN paradigm, since DDoS attacks are one of the biggest threats that software defined networks can face due to their architecture[1].

As part of this survey, we provide a thorough review and comparison of the existing attack models that could be applied to SDN. After the analysis and simulations we carried out, we found that it is possible to adapt the Congestion Window, Queuing and Epidemic model to SDN due to the similar behaviour and protocols that they contemplate. It is possible to apply these models to software defined networks because SDN networking devices can also be exhausted in similar ways, the main difference relies on how traffic is processed between the different planes in SDN, so it is required to adapt the models. One more reason why the models can be applied to SDN is because OpenFlow uses TCP, where controllers listen on TCP port 6653 [95] to establish communications with SDN networking devices. As future work we plan to adapt the aforementioned models to SDN in order to study which additional parameters are required to be considered and simulate the models to verify how close the model behaves with the real testbed.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

Juan Balarezo and Song Wang are supported by the Australian Government Research Training Program Scholarship.

The authors would like to thank the editors and anonymous reviewers for providing insightful suggestions and comments to improve the quality of research paper.

References

[1] ETSI, Network Functions Virtualisation (NFV): Architectural Framework, ETSI, 2014, Accessed:15/10/2020. URL: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf.

[2] T. Benson, A. Akella, D.A. Maltz, Unraveling the Complexity of Network Management, in: Networked Systems Design and Implementation (NSDI), 2009, pp. 335–348.

[3] D. Kreutz, F.M.V. Ramos, P.E. Veríssimo, C.E. Rothenberg, S. Azodolmolky, S. Uhlig, Software-Defined Networking: A Comprehensive Survey, Proceedings of the IEEE 103 (1) (2015) 14–76, https://doi.org/10.1109/JPROC.2014.2371999.

[4] R. Von Solms, J. Van Niekerk, From information security to cyber security, Computers & Security 38 (2013) 97–102, https://doi.org/10.1016/j.cose.2013.04.004.

[5] NETSCOUT, NETSCOUT Arbor's 14th Annual Worldwide Infrastructure Security Report (WISR), NETSCOUT, 2019, Accessed:21/11/2020. URL: https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf.

[6] R. Maciel, J. Araujo, J. Dantas, C. Melo, E. Guedes, P. Maciel, Impact of a DDoS attack on computer systems: An approach based on an attack tree model, in: International Systems Conference (SysCon), IEEE, 2018, pp. 1–8..

[7] S. Ramanauskaitė, A. Cenys, N. Goranin, J. Janulevicius, Modeling of two-tier DDoS by combining different type of DDoS models, in: Conference of Electrical, Electronic and Information Sciences (eStream), 2017, pp. 1–4..

[8] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, K. Long, On a Mathematical Model for Low-Rate Shrew DDoS, IEEE Transactions on Information Forensics and Security 9 (7). doi:10.1109/TIFS.2014.2321034..

[9] Y. Xiang, Z. Li, An Analytical Model for DDoS Attacks and Defense, in: Conference on Computing in the Global Information Technology, 2006, p. 66.

[10] S. Ramanauskaitė, N. Goranin, A. Čenys, J. Juknius, Modelling influence of Botnet features on effectiveness of DDoS attacks, Security and Communication Networks 8 (12) (2015) 2090–2101, https://doi.org/10.1002/Section 1156.

[11] M. Eian, S.F. Mjølsnes, The modeling and comparison of wireless network Denial of Service attacks, in: ACM Symposium on Operating Systems Principles (SOSP) workshop, ACM, 2011, p. 7..

[12] U. Kumar, S.K. Pandey, Dynamic Model on DDoS Attack in Computer Network, in: ACM Conference on Information and Analytics ACM, 2016, pp. 1–5.

[13] X. Wang, M. Chen, C. Xing, SDSNM: A Software-Defined Security Networking Mechanism to Defend against DDoS Attacks, in: Conference on Computer Science and Technology, 2015..

[14] B. Yuan, D. Zou, S. Yu, H. Jin, W. Qiang, J. Shen, Defending Against Flow Table Overloading Attack in Software-Defined Networks, IEEE Transactions on Services Computing 12 (2) (2019) 231–246, https://doi.org/10.1109/TSC.2016.2602861.

[15] C. Chung, P. Khatkar, T. Xing, J. Lee, D. Huang, NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems, IEEE Transactions on Dependable and Secure Computing 10 (4) (2013) 198–211, https://doi.org/10.1109/TDSC.2013.8.

[16] Z. Li, H. Jin, D. Zou, B. Yuan, Exploring New Opportunities to Defeat Low-Rate DDoS Attack in Container-Based Cloud Environment, IEEE Transactions on Parallel and Distributed Systems 31 (3) (2020) 695–706, https://doi.org/10.1109/TPDS.2019.2942591.

[17] M.N. Rajkumar, A survey on latest DoS attacks: classification and defense mechanisms, Journal of Innovative Research in Computer and Communication Engineering 1 (8) (2013) 1847–1860.

[18] M. Dabbagh, B. Hamdaoui, M. Guizani, A. Rayes, Software-Defined Networking security: pros and cons, IEEE Communications Magazine 53 (6) (2015) 73–79, https://doi.org/10.1109/MCOM.2015.7120048.

[19] K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui, Software-Defined Networking (SDN): a survey, Security and Communication Networks 9 (18) (2016) 5803–5833. doi:10.1002/Section 1737..

[20] S.T. Zargar, J. Joshi, D. Tipper, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials 15 (4) (2013) 2046–2069, https://doi.org/10.1109/SURV.2013.031413.00127.

[21] A. Furfaro, G. Malena, L. Molina, A. Parise, A Simulation Model for the Analysis of DDoS Amplification Attacks, in: Conference on Modelling and Simulation, 2015, pp. 267–272.

[22] K.S. Bhosale, M. Nenova, G. Iliev, The Distributed Denial of Service attacks (DDoS) prevention mechanisms on application layer, in: Conference on Advanced Technologies, Systems and Services in Telecommunications, IEEE, 2017, pp. 136–139.

[23] A. Praseed, P.S. Thilagam, DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications, IEEE Communications Surveys & Tutorials 21 (1) (2019) 661–685, https://doi.org/10.1109/COMST.2018.2870658.

[24] NETSCOUT, NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report (WISR), NETSCOUT, 2018, Accessed:14/02/2019. URL: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf.

[25] N. Dayal, P. Maity, S. Srivastava, R. Khondoker, Research trends in security and DDoS in SDN, Security and Communication Networks 9 (18) (2016) 6386–6411, https://doi.org/10.1002/Section 1759.

[26] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, OpenFlow: Enabling innovation in campus networks, ACM Special Interest Group on Data Communications (SIGCOMM) Computer Communication Review 38 (2) (2008) 69–74. doi:10.1145/1355734.1355746..

[27] A. Blenk, A. Basta, M. Reisslein, W. Kellerer, Survey on Network Virtualization Hypervisors for Software Defined Networking, IEEE Communications Surveys & Tutorials 18 (1) (2016) 655–685, https://doi.org/10.1109/COMST.2015.2489183.

[1] Scripts used for the simulations are available at: https://github.com/juanferbal?tab=repositories

[28] W. Yang, C. Fung, A survey on security in Network Functions Virtualization, in: IEEE Network Softwarization (NetSoft) Conference and Workshops, IEEE, 2016, pp. 15–19..
[29] ETSI, Network Functions Virtualisation (NFV): Infrastructure Overview, ETSI, 2015, Accessed:15/10/2020. URL: https://www.etsi.org/deliver/etsi_gs/nfv-inf/001_099/001/01.01.01_60/gs_nfv-inf001v010101p.pdf.
[30] ETSI, Network Functions Virtualisation (NFV): Virtual Network Functions Architecture, ETSI, 2014, Accessed:15/10/2020. URL: https://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf.
[31] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, A. Meddahi, NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures, IEEE Communications Surveys & Tutorials 20 (4) (2018) 3330–3368, https://doi.org/10.1109/COMST.2018.2859449.
[32] P. Sheinidashtegol, M. Galloway, Performance Impact of DDoS Attacks on Three Virtual Machine Hypervisors, in: International Conference on Cloud Engineering (IC2E), 2017, pp. 204–214.
[33] F.Z. Yousaf, M. Bredel, S. Schaller, F. Schneider, NFV and SDN–Key Technology Enablers for 5G Networks, IEEE Journal on Selected Areas in Communications 35 (11) (2017) 2468–2478, https://doi.org/10.1109/JSAC.2017.2760418.
[34] ONF, Relationship of SDN and NFV, ONF, 2015, Accessed:10/10/2020. URL: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/onf2015.310_Architectural_comparison.08-2.pdf..
[35] ETSI, Network Functions Virtualisation (NFV) Ecosystem: Report on SDN Usage in NFV Architectural Framework, ETSI, 2015, Accessed:10/10/2020. URL: https://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_nfv-eve005v010101p.pdf.
[36] M.V. De Assis, A.H. Hamamoto, T. Abrão, M.L. Proença, A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks, IEEE Access 5 (2017) 9485–9496, https://doi.org/10.1109/ACCESS.2017.2702341.
[37] S.M. Tabatabaie Nezhad, M. Nazari, E.A. Gharavol, A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks, IEEE Communications Letters 20 (4) (2016) 700–703. doi:10.1109/LCOMM.2016.2517622..
[38] J. Zheng, A.S. Namin, Defending SDN-based IoT Networks Against DDoS Attacks Using Markov Decision Process, in: IEEE International Conference on Big Data, 2018, pp. 4589–4592.
[39] K. Kalkan, L. Altay, G. Gür, F. Alagöz, JESS: Joint Entropy-Based DDoS Defense Scheme in SDN, IEEE Journal on Selected Areas in Communications 36 (10) (2018) 2358–2372, https://doi.org/10.1109/JSAC.2018.2869997.
[40] L. Dridi, M.F. Zhani, A holistic approach to mitigating DoS attacks in SDN networks, International Journal of Network Management 28 (1) (2018), https://doi.org/10.1002/nem.1996 e1996.
[41] A. Chonka, J. Singh, W. Zhou, Chaos theory based detection against network mimicking DDoS attacks, IEEE Communications Letters 13 (9) (2009) 717–719, https://doi.org/10.1109/LCOMM.2009.090615.
[42] D. Yin, L. Zhang, K. Yang, A DDoS attack detection and mitigation with software-defined Internet of Things framework, IEEE Access 6 (2018) 24694–24705, https://doi.org/10.1109/ACCESS.2018.2831284.
[43] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, Scale inside-out: Rapid mitigation of cloud DDoS attacks, IEEE Transactions on Dependable and Secure Computing 15 (6) (2018) 959–973, https://doi.org/10.1109/TDSC.2017.2763160.
[44] K. Hong, Y. Kim, H. Choi, J. Park, SDN-assisted slow HTTP DDoS attack defense method, IEEE Communications Letters 22 (4) (2018) 688–691, https://doi.org/10.1109/LCOMM.2017.2766636.
[45] A. Sahi, D. Lai, Y. Li, M. Diykh, An efficient DDoS TCP flood attack detection and prevention system in a cloud environment, IEEE Access 5 (2017) 6036–6048, https://doi.org/10.1109/ACCESS.2017.2688460.
[46] N. Hoque, D.K. Bhattacharyya, J.K. Kalita, Botnet in DDoS attacks: trends and challenges, IEEE Communications Surveys & Tutorials 17 (4) (2015) 2242–2270, https://doi.org/10.1109/COMST.2015.2457491.
[47] Z. Liu, H. Jin, Y.-C. Hu, M. Bailey, Practical proactive DDoS-attack mitigation via endpoint-driven in-network traffic control, IEEE/ACM Transactions on Networking 26 (4) (2018) 1948–1961, https://doi.org/10.1109/TNET.2018.2854795.
[48] B. Rashidi, C. Fung, E. Bertino, A Collaborative DDoS Defence Framework Using Network Function Virtualization, IEEE Transactions on Information Forensics and Security 12 (10) (2017) 2483–2497, https://doi.org/10.1109/TIFS.2017.2708693.
[49] S.B. Alaoui, T. El Houssaine, C. Noreddine, Modelling, analysis and design of active queue management to mitigate the effect of Denial of Service attack in wired/wireless network, in: International Conference on Wireless Networks and Mobile Communications (WINCOM) IEEE, 2019, pp. 1–7.
[50] W. Yong, S.H. Tefera, Y.K. Beshah, Understanding Botnet: From Mathematical Modelling to Integrated Detection and Mitigation Framework, in: International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2012, pp. 63–70..
[51] Qiang Huang, H. Kobayashi, Bede Liu, Modeling of Distributed Denial of Service attacks in wireless networks, in: Pacific Rim Conference on Communications Computers and Signal Processing (PACRIM), Vol. 1, IEEE, 2003, pp. 41–44 vol 1..
[52] Y. Wang, C. Lin, Q.-L. Li, Y. Fang, A queuing analysis for the denial of service (DoS) attacks in computer networks, Computer Networks 51 (12) (2007) 3564–3573, https://doi.org/10.1016/j.comnet.2007.02.011.
[53] D.K. Saini, S.A. Maskari, H. Saini, Malicious objects trafficking in the network, in: International Conference on Digital Content, Multimedia Technology and its Applications, 2011, pp. 64–69..
[54] G. Vormayr, T. Zseby, J. Fabini, Botnet communication patterns, IEEE Communications Surveys & Tutorials 19 (4) (2017) 2768–2796, https://doi.org/10.1109/COMST.2017.2749442.
[55] M. de la Sen, S. Alonso-Quesada, A. Ibeas, A SIS epidemic model with impulsive vaccination, in: Conference on Industrial Engineering and Engineering Management, IEEE, 2013, pp. 1156–1161.
[56] V. Matta, M. Di Mauro, M. Longo, A. Farina, Cyber-Threat Mitigation Exploiting the Birth-Death-Immigration Model, IEEE Transactions on Information Forensics and Security 13 (12) (2018) 3137–3152, https://doi.org/10.1109/TIFS.2018.2838084.
[57] M.T. Gardner, C. Beard, D. Medhi, Using SEIRS Epidemic Models for IoT Botnets Attacks, in: Design of Reliable Communication Networks (DRCN) International Conference, 2017, pp. 1–8..
[58] K.Y. Nikolskaya, S.A. Ivanov, V.A. Golodov, A.S. Sinkov, Development of a mathematical model of the control beginning of DDoS-attacks and malicious traffic, in: International Conference Quality Management,Transport and Information Security, Information Technologies (IT QM IS), IEEE, 2017, pp. 84–86.
[59] X. Ma, Y. Chen, DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy, IEEE Communications Letters 18 (1) (2014) 114–117, https://doi.org/10.1109/LCOMM.2013.112613.132275.
[60] A. Chonka, J. Singh, W. Zhou, Chaos theory based detection against network mimicking DDoS attacks, IEEE Communications Letters 13 (9) (2009) 717–719, https://doi.org/10.1109/LCOMM.2009.090615.
[61] N. Jeyanthi, J. Vinithra, R. Sneha, N.C.S.N. Iyengar Thandeeswaran, A Recurrence Quantification Analytical Approach to Detect DDoS Attacks, in: International Conference on Computational Intelligence and Communication Networks IEEE, 2011, pp. 58–62.
[62] Y. Tao, S. Yu, DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics, in: International Conference on Trust, Security and Privacy in Computing and Communications IEEE, 2013, pp. 233–240.
[63] A. Gaurav, A.K. Singh, Entropy-score: A method to detect DDoS attack and flash crowd, in: International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), IEEE, 2017, pp. 1427–1431..
[64] R.F. Fouladi, O. Ermis, E. Anarim, Anomaly-Based DDoS Attack Detection by Using Sparse Coding and Frequency Domain, in: International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2019, pp. 1–6.
[65] T. Thapngam, S. Yu, W. Zhou, G. Beliakov, Discriminating DDoS attack traffic from flash crowd through packet arrival patterns, in: Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2011, pp. 952–957.
[66] H. Yang, R. Jiang, C. Zhao, A. Li, Evaluation of DDOS Attack Degree Based on GRA-TOPSIS Model, in: International Conference on Smart Grid and Electrical Automation (ICSGEA), IEEE, 2019, pp. 547–552.
[67] H. Lin, S. Cao, J. Wu, Z. Cao, F. Wang, Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices, IEEE Access 7 (2019) 164480–164491, https://doi.org/10.1109/ACCESS.2019.2950820.
[68] A. Abhishta, R. Joosten, S. Dragomiretskiy, L.J.M. Nieuwenhuis, Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange, in: Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), IEEE, 2019, pp. 379–384..
[69] T. Babenko, S. Toliupa, Y. Kovalova, LVQ models of DDOS attacks identification, in: International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), IEEE, 2018, pp. 510–513..
[70] S. Yamaguchi, H. Tanaka, Modeling of Infection Phenomenon and Evaluation of Mitigation Methods for IoT Malware Mirai by Agent-Oriented Petri Net PN2, in: International Conference on Consumer Electronics-Taiwan (ICCE-TW), IEEE, 2018, pp. 1–2..
[71] R.C. Diovu, J.T. Agee, Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks, in: International Conference on Electro-Technology for National Development (NIGERCON), IEEE, 2017, pp. 696–701.
[72] U. Yatsykovska, M. Karpinski, I. Vasyltsov, P. Bykovyy, The monitoring system of DoS/DDoS attacks in the global network, in: Proceedings of the 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, Vol. 2, IEEE, 2011, pp. 791–794..
[73] D. Sattar, A. Matrawy, Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices, in: Conference on Communications and Network Security (CNS), IEEE, 2019, pp. 82–90.
[74] E.S.C. Vilaça, T.P.B. Vieira, R.T. de Sousa, J.P.C.L. da Costa, Botnet traffic detection using RPCA and Mahalanobis Distance, in: Workshop on Communication Networks and Power Systems (WCNPS), IEEE, 2019, pp. 1–6..
[75] P. Cheskidov, K. Nikolskaia, A. Minbaleev, Choosing the Reinforcement Learning Method for Modeling DDoS Attacks, in: International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), IEEE, 2019, pp. 1–4..
[76] P. Holgado, V.A. Villagrá, L. Vázquez, Real-Time Multistep Attack Prediction Based on Hidden Markov Models, IEEE Transactions on Dependable and Secure Computing 17 (1) (2020) 134–147, https://doi.org/10.1109/TDSC.2017.2751478.
[77] M.D. Mauro, G. Galatro, A. Liotta, Experimental Review of Neural-Based Approaches for Network Intrusion Management, IEEE Transactions on

Network and Service Management 17 (4) (2020) 2480–2495, https://doi.org/10.1109/TNSM.2020.3024225.
[78] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del Rincón, D. Siracusa, Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection, IEEE Transactions on Network and Service Management 17 (2) (2020) 876–889. doi:10.1109/TNSM.2020.2971776..
[79] B. Hussain, Q. Du, B. Sun, Z. Han, Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System Over 5G Network, IEEE Transactions on Industrial Informatics 17 (2) (2021) 860–870, https://doi.org/10.1109/TII.2020.2974520.
[80] V. Matta, M. Di Mauro, M. Longo, Botnet identification in multi-clustered DDoS attacks, in: European Signal Processing Conference (EUSIPCO), 2017, pp. 2171–2175.
[81] L. Shi, J. Li, M. Zhang, P. Reiher, On Capturing DDoS Traffic Footprints on the Internet, IEEE Transactions on Dependable and Secure Computing (2021) 1, https://doi.org/10.1109/TDSC.2021.3074086.
[82] A. Sangodoyin, B. Mohammed, M. Sibusiso, I. Awan, J.P. Disso, A Framework for Distributed Denial of Service Attack Detection and Reactive Countermeasure in Software Defined Network, in: International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2019, pp. 80–87.
[83] R. Wang, Z. Jia, L. Ju, An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking, in: Trustcom/BigDataSE/ISPA, Vol. 1, IEEE, 2015, pp. 310–317. doi:10.1109/Trustcom.2015.389..
[84] N. Dayal, S. Srivastava, Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN, in: International Conference on Communication Systems and Networks (COMSNETS), IEEE, 2017, pp. 274–281.
[85] J. Zheng, A.S. Namin, Defending SDN-based IoT Networks Against DDoS Attacks Using Markov Decision Process, in: International Conference on Big Data (Big Data), IEEE, 2018, pp. 4589–4592..
[86] X. Yang, B. Han, Z. Sun, J. Huang, SDN-Based DDoS Attack Detection with Cross-Plane Collaboration and Lightweight Flow Monitoring, in: GLOBECOM Global Communications Conference, IEEE, 2017, pp. 1–6.
[87] Y. Liu, M. Dong, K. Ota, J. Li, J. Wu, Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software-Defined Networks, in: International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2018, pp. 1–6..
[88] V. Deepa, K.M. Sudar, P. Deepalakshmi, Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques, in: International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 2018, pp. 299–303.
[89] K.S. Sahoo, B.K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, D. Burgos, An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks, IEEE Access 8 (2020) 132502–132513, https://doi.org/10.1109/ACCESS.2020.3009733.
[90] A. Girma, M. Garuba, J. Li, C. Liu, Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment, in: International Conference on Information Technology - New Generations, IEEE, 2015, pp. 212–217..
[91] S. Yu, Y. Tian, S. Guo, D.O. Wu, Can We Beat DDoS Attacks in Clouds?, IEEE Transactions on Parallel and Distributed Systems 25 (9) (2014) 2245–2254, https://doiorg/10.1109/TPDS.2013.181.
[92] T.V. Phan, M. Park, Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud, IEEE Access 7 (2019) 18701–18714, https://doi.org/10.1109/ACCESS.2019.2896783.
[93] R. Biswas, S. Kim, J. Wu, Sampling Rate Distribution for Flow Monitoring and DDoS Detection in Datacenter, IEEE Transactions on Information Forensics and Security 16 (2021) 2524–2534, https://doi.org/10.1109/TIFS.2021.3054522.
[94] B.F. Maier, D. Brockmann, Effective containment explains subexponential growth in recent confirmed COVID-19 cases in China, Science 368 (6492) (2020) 742–746, https://doi.org/10.1126/science.abb4557.
[95] ONF, OpenFlow Switch Specification Version 1.5.1, ONF (2015). Accessed:10/10/2020. URL: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.