IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 March 2023, accepted 10 May 2023, date of publication 15 May 2023, date of current version 5 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3276238

SURVEY

A Systematic Literature Review of Offensive and Defensive Security Solutions With Software Defined Network

ANDREA MELIS, AMIR AL SADI, DAVIDE BERARDI, FRANCO CALLEGATI, (Senior Member, IEEE), AND MARCO PRANDINI, (Member, IEEE)
Department of Computer Science and Engineering, University of Bologna, 40126 Bologna, Italy
Corresponding author: Andrea Melis (a.melis@unibo.it)

ABSTRACT Software Defined Networking (SDN) is one of the most significant innovations in telecommunication systems in the past two decades. From the very beginning, the scientific community understood the importance of investigating the possible usages of SDN as a means to increase network security, but also their potential to be exploited as an attack device. For this reason, there has been a massive production of research works, which, however, do not form a well-defined corpus. The literature is spread over many venues and composed of contributions with very different flavors. Though some review works already exist, in this work we conduct a systematic literature review of the field, gathering 466 relevant publications—the largest curated dataset on the topic to the best of our knowledge. In our work, the dataset undergoes a twofold analysis: (a) quantitative, through publication metadata, which allows us to chart publication outlets, approaches, and tackled issues; (b) qualitative, through 14 research questions that provide an aggregated overview of the literature contributions to the key issues, also to spot gaps left open. From these analyses, we derive a call for action to address the main open challenges.

INDEX TERMS Attack, defense, mitigation, security, SDN, threat.

I. INTRODUCTION

The level of complexity of modern communications, as well as their key role in our daily life, calls for outstanding levels of performance, reliability, and security. The TCP/IP protocol suite provided the basic technology for the widespread development of the Internet. Still, it was not designed to cope with the huge variety of use cases of today. The consequence was inevitably the ''ossification'' of the Internet, which has been overcome with the introduction of a number of additional devices performing several ancillary functions, the so-called middleboxes. The explosion of the number of middleboxes hinders effective management, smooth scalability, as well as controllable security of the network.

The Software Defined Networking (SDN) principle emerged with the goal to overcome these problems. It allows full decoupling between the network control and data planes, to allow full flexibility in functional evolution and guarantee scalability. Moreover, it allows network reconfiguration and adaptation to different application scenarios and operating conditions, within a time scale unforeseeable with legacy technologies. The SDN operates according to the model of a control plane implemented with *controllers* that communicate with *switches* implementing the data plane and are physically responsible for forwarding messages along the network. The communication between control and data planes can be implemented in various ways; nowadays, the de-facto standard is Openflow [15], and an SDN-enabled switch has one or more flow tables, configured by the SDN controller via the OpenFlow API. In normal operations, a flow table contains rules that match a given packet header with common networking actions such as prioritization, queuing, packet switching, etc. Besides the split between control and data planes, SDN brings forward two additional significant innovations, that are:

The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Mueen Uddin.

- a flow may typically be identified by a subset of the packet header field that may belong to different protocol layers (for instance IP source and destination and some combination of TCP/UDP ports);
- forwarding rules may change over time as the controller dynamically makes new decisions on how to route individual flows, possibly reacting to some sort of network behavior.

The SDN approach attracted a lot of interest from both the academic and industrial communities in the last two decades [25]. The ability of this type of architecture to easily adapt to a particular scenario has made SDN a widely used technology to model complex network attack detection and mitigation solutions, but also, albeit less frequently, to orchestrate effective attack campaigns. The goal of this manuscript is to extensively analyze the state of the art regarding SDN security-related research from both defensive and offensive security points of view. We used the methodology of systematic literature review in order to obtain an overview of the main research trends. By studying a large number of papers that treat this topic, we identified the most relevant SDN usage scenarios, considering the common practice, implementation standards, or threat modeling methods. Furthermore, we tried to identify the correlations between SDN security and other developing technologies, such as Network Function Virtualization (NFV) and Machine Learning (ML).

This work is structured as follows:

- After this introduction, Section II lists the related works for the SDN security field and the state of the art in terms of systematic literature review.
- Section III describes the preliminary phase of the work, which is data collection. It describes the source querying and the publication gathering process, as well as the selection criteria.
- Section IV enunciates the research questions, which is the starting point for the qualitative analysis of the selected publications.
- Section V presents the results of the literature revision, providing both qualitative and quantitative information, giving priority to the qualitative ones which are the main goal of this work.
- In Section VI-B, the correlations between articles' keywords found in the abstracts and the correlations between research questions are presented, to highlight the main connected topics.
- Final remarks are presented in Section VII, with a particular focus on the open challenges we found to be relevant during the writing of this literature review.
- The last Section VIII provides overall observations and final conclusions.

II. RELATED WORK

There are some works that provide classic survey/review of offensive and defensive security applications of SDN. The main difference with the present work is that they either do not use a systematic approach or are not as general and comprehensive.

In fact, many reviews focus vertically on DDoS attack detection or mitigation, not considering other types of attacks or threats. Relevant works include:

Authors in [18] reviewed around 70 DDoS detection and mitigation mechanisms in SDN networks and discussed challenges to developing defense mechanisms for DDoS attacks. As far as we know this is the published work that is closest to this manuscript since the majority of the current literature (as it will be pointed out in section V-B2) focuses on DDoS detection. This is the only systematic review that is partially close to our proposed work.

In [2] otherwise authors proposed a survey about DoS and DDoS mitigation techniques in SDN. This work categorizes DoS in SDN into two groups: DoS attacks in SDN and SDN-based solutions to tackle DoS attacks in the networks.

In [9] authors presented a survey about DDoS attacks in SDN and Cloud Computing architectures. In section IV, the authors outline the tools mostly used in SDN and Cloud Computing. We believe that an important driving factor in SDN research is the presence of a few largely used technologies.

In [12] a literature review is presented, regarding various DDoS defense mechanisms to protect against attacks at every level in the SDN. Furthermore, a taxonomy of DDoS defense mechanisms is presented, based on attack targets.

Although these works proved to be well received and have been the inspiration for our review, we argue that they lack a more in-depth horizontal analysis of all possible SDN threats and attacks.

For this reason, we considered also some related work that tried to have a wider analysis of the security threats on SDN.

In [7] authors listed vulnerabilities and information security threats in SDN. This survey first divides threats into the control plane, data plane, and host/channel vulnerabilities and then proceeds to list information security issues and possible countermeasures to guarantee confidentiality, authenticity, integrity, consistency, and availability.

In [ds169] authors otherwise tackled the problem of SDN security issues classification according to the STRIDE threat model categories.

In [ds81] authors described a set of threats and vulnerabilities in SDNs derived by intrinsic problems of the paradigm or misconfigurations.

In [27] authors presented a survey on cyber-defense measures developed using SDN. This survey includes malware and social engineering as attack vectors. In this survey, the interesting topic is social engineering, which declined in the flavor of phishing.

There are also surveys that analyze the security of the control plane, in terms of infrastructure configuration which is something that we also evaluated in our work; e.g.:

In [1] a survey that analyzes the decentralization of different SDN controllers is proposed. Other than this, the manuscript goes through a number of different parameters which comprise security.

In [ds138] otherwise an analysis of the main threats and vulnerabilities of SDN controlled IoT environment, at the control plane, is performed.

Also, the scientific community proposes works that aim to review existing SDN-based solutions to detect and react to attacks with state-of-the-art paradigms such as NFV and ML.

In [11] for example authors presented a survey that analyzes strategies to monitor, protect and react to IoT threats. The authors believe that security solutions that combine SDN and NFV are not often considered in the literature but there are several advantages (in terms of scalability, on-demand network programmability, energy efficiency, and mobility support) to revert this trend.

In [21] finally a review is shown evaluating techniques of Machine Learning/deep learning used to develop SDN-based NIDS models. The authors believe that with the help of ML/DL, SDN-based NIDS can be used in critical infrastructures.

Although literature that tackles certain specific topics of SDN is rich and established, we argue that there is no **comprehensive** and **systematic** literature review on offensive and defensive cybersecurity solutions based on SDN.

The related works that we discussed did not use a systematic approach or did not include the different aspects of cybersecurity. We believe that the maturity of the SDN paradigm makes it relevant and strongly justifies a systematic analysis of the literature.

However, to our knowledge, a systematic literature review about SDN Security solutions both from an offensive or defensive point-of-view has not been realized yet.

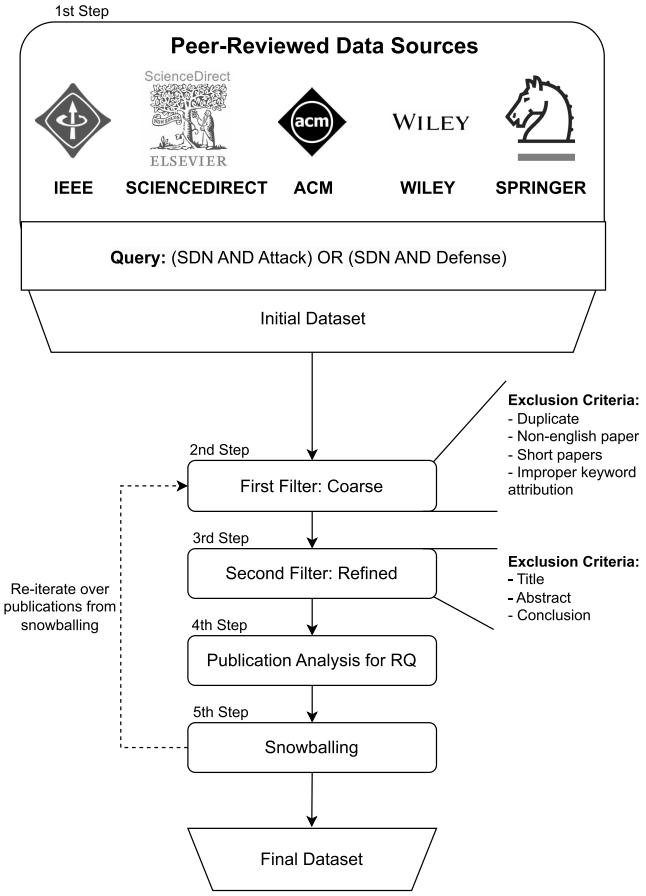


FIGURE 1. Schema of the method followed to gather the dataset for this survey.

III. REVIEW METHOD

In this section, we describe the methodology of our systematic review. Following the guidelines by [19], and as depicted in Fig. 1, we started by searching and retrieving the literature for relevant publications from several data sources by using the same keyword query. We then performed a manual revision process of the automatically selected publications to exclude those that fall out of the scope of this study. The resulting dataset consists of 466 publications. We analyzed these publications to collect statistical and objective answers to our research questions, which are detailed in Section IV.[1]

A. SELECTION QUERY AND COLLECTION OF PUBLICATIONS

In the literature, we can find many security aspects related to SDN. In several cases, these aspects are also part of wider application contexts such as Blockchain and Edge Computing. For this reason, the use of the query "sdn AND security" produced more than ten thousand papers, an amount that would make it a daunting task to find any meaningful insight.

We, therefore, opted for a more restrictive query:

"(sdn AND attack) OR (sdn AND defense)".

[1]The list of the publications and their bibliography information is publicly available at https://doi.org/10.5281/zenodo.6959369

In this work we focus on papers that propose specific solutions, entailing the usage of SDN for offensive or defensive purposes. Accordingly, we looked at how SDN can be used to create infrastructure to perform attacks or to create or host defense mechanisms.

Given the potential unmanageable size of the data set, an additional pre-selection criterion we adopted was to consider white literature only: in terms of quantity, it represents a very meaningful sample of the research produced during the considered time frame, and in terms of quality, it allowed us to rely on peer-reviewed papers only. Thanks to the more uniform organization of white literature, we are also more confident in the level of consistency of our choice and application of the selection criteria. This is not to say that grey literature is not worth investigating. Blog posts, personal websites, technical reports, white papers, etc., are often the preferred venues for practitioners to share ideas. However, as also pointed out in [20], "it is very difficult to uniquely measure the quality of grey literature when conducting a systematic, controllable, and replicable secondary study" and we are not aware of a standard method for the evaluation of grey literature.

It was also decided to limit the search to papers published from 2015 onwards. We have therefore collected 3494 papers, coming from 5 distinct sources:

TABLE 1. Related work classification based on the topic.

Category	Description	Articles
SDN	Review or Survey about SDN Security vulnerabilities and defence mechanisms	[bb7], [ds169], [bb27], [ds81], [bb21]
SDN + Other Topic	Review or Survey about SDN and another topic combined	[bb1] (SDN and controller decentralization) [ds138] (SDN Security and IoT) [bb11] (SDN Security and NFV)
DDoS	DDoS attacks and defence mechanisms against SDN architectures	[bb2], [bb12], [bb12], [bb9]

- ACM (https://dl.acm.org/), 776 paper;
- IEEE Explore (https://ieeexplore.ieee.org/), 940 paper;
- Science Direct (https://www.sciencedirect.com/), 1143 paper;
- Wiley (https://onlinelibrary.wiley.com/), 192 paper;
- Springer (https://link.springer.com//), 443 paper.

The publications were collected up to December 2021, using the academic subscriptions provided by the University affiliation of the authors.

B. PUBLICATION TRIAGE

The publications obtained from the process described above were further reviewed in two steps, each consisting of different exclusion criteria. During the first step, for each paper, we checked the presence and frequency of the search keywords *SDN, Attack* and *Defense* in the text. We discarded the papers characterized by a small and irrelevant use of the above keywords, i.e. those with less than 4 occurrences of the term *SDN* or both of the terms *Attack-Defense*. We have also removed the papers in which the terms are mentioned exclusively in the bibliography and those where the keywords are interpreted in a different way than intended.

We then discarded publications not written in English and those consisting of less than 4 pages. Lastly, we proceeded to eliminate any duplicate papers, received from more than one data source.

In the second step, we performed an analysis of the title, the abstract, and the conclusions of each publication and we discarded the papers where the SDN or the Security topic was just orthogonal to the main paper goal.

Summarizing, we performed a paper filtering operation based on the following exclusion criteria (**E**i):

- E1: The paper includes parts about SDN, although this is not the central topic;
- E2: The security of SDN, in terms of attacks or defense measures, is not a topic of the paper, or it is not the main one;
- E3: In the body of the paper there are less than 4 occurrences of search keywords *Attack* and *Defense*;
- E4: The concatenated text of the title, abstract, and conclusions does not present any of the search keywords.

At the end of this process, we then obtained a final dataset of 466 papers, distributed across the following publishers:

- ACM (Digital Library – https://dl.acm.org/), 96 papers;
- IEEE (IEEExplore – https://ieeexplore.ieee.org/), 190 papers;
- Elsevier (Science Direct – https://www.sciencedirect.com/), 68 papers;
- Wiley (Online Library – https://onlinelibrary.wiley.com/), 40 papers;
- Springer (Online Library –link.springer.com/), 72 paper.

IV. RESEARCH QUESTIONS

In this section, we present the research questions that guided our systematic review.

Usually, the research questions for systematic literature reviews are fairly broad and not more than six. In our study, we chose to adopt more questions (14) but mostly dichotomous (i.e., with yes-or-no answers), with the goal of favoring precision and objectiveness.

To define the questions and seek guidance in categorizing the relevant security issues for SDN and Security, we took inspiration from the related work presented II, as well as from the state of the art in standards and methodologies such as [23]. We grouped the research questions into 4 groups (**G**i):

- G1: Threat Model. Questions on how to classify and identify threats.
- G2: Security approach. Questions about the security approach adopted, for example, whether threat prevention, identification, or mitigation mechanisms are used.
- G3: Infrastructure. Questions on the infrastructure study subject.
- G4: Primary goal. Questions on the main purpose of the paper being studied.

A. FIRST GROUP: THREAT MODEL

Mapping the usage of threat models is important to see gaps when a security the violation must be handled, or if known models are outdated and need to be adjusted. The usage of a formal threat model has proven to be extremely useful in the identification of attack types and their strategic countermeasures [6].

Several threat models exist in the literature. The most famous one is STRIDE [13] named after the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege security threats. Other threat models however exist, such as PASTA [24] or OWASP [16].

In our review and with this first group of questions, we aimed to understand whether a publication fol-

lowed a known model, strategy, or guideline. Alternatively, we wanted to know if new security models were proposed. This group is composed of the following questions:

- Q1: Does the paper consider STRIDE aspects?
- Q2: Even without explicitly mentioning STRIDE, does it involve at least one of its features such as:
  - Spoofing
  - Tampering
  - Authentication and Authorization
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service
  - Elevation of privilege
- Q3: If considered, does the paper propose/discuss a concrete implementation/solution developed by the same author or just one taken from the literature?
- Q4: Does the paper consider, propose or follow another relevant threat model rather than STRIDE or some proposed by the same authors? (e.g. PASTA., or any other threat modeling by design approach)
- Q5: Does the paper mention policies/workflows/guidelines to handle violations?

B. SECOND GROUP: GENERAL APPROACH

Securing a network of computers is a complex process that has numerous aspects to take into consideration. The second group of questions aims to provide a more detailed picture of the implemented functionalities and approaches adopted in the literature concerning this study.

This group is composed of the following questions:

- Q6: Is the paper mentioning IDS functionalities?
- Q7: Is the paper mentioning IPS functionalities?
- Q8: Is the paper mentioning Threat Intelligence?
- Q9: Is the paper mentioning Exfiltration Leaks?
- Q10: Does the paper approach/address insider threats?

C. THIRD GROUP: INFRASTRUCTURE

The SDN approach provides *by design* extensive integration with complementary architectures, such as NFV, which allow the entire network to be virtualized, providing centralized control and orchestration capabilities; there is also the possibility, during the implementation phase of the network, to make use of existing software components. This fourth group's questions aim to obtain a detailed classification of the infrastructures proposed in the selected papers.

This group is composed of the following questions:

- Q11: Does the paper use NFV management/orchestration?
- Q12: Does the paper mention known technologies such as:
  - Onos
  - Ryu
  - Open Source Mano
  - Mininet
  - P4 language
- Q13: Does the paper mention/use Machine Learning techniques?

Insights

Insights: In the following subsections, we highlight in boxes (like this one) the main insights that emerge from our analysis. From each insight, an open challenge ensues, which we summarize in a bold typeface at the start of its description. We will use these challenges in Section V to structure our discussion about useful future directions for research on SDN security.

D. FOURTH GROUP: MOTIVATION

Finally, the fourth group focuses on the purpose of the publications under review, examining whether there are research trends in a specific context or relative to a specific category of attacks.

This group is composed only of one question, aimed to look if the paper studies a specific attack type:

- Q14: Is it a paper focused on a specific attack?

The motivation for defining this last question comes from the fact that, based on our experience, we expected a predominance of jobs dedicated to denial of service. Consequently, the question aimed to select the paper where there is a clear attack type studied, and then we used such information to categorize also the attacks. These results are reported in detail in section V-B1.

V. REVIEW RESULTS

In this section, we present the results of the literature review. We start by presenting quantitative results from the metadata of the publications in the dataset. This is useful to map the trends of the research over time as well as the current shape of the field, in terms of the number of contributions, type (proceedings, articles), communities, and keywords. This is followed by a qualitative analysis which aims at providing a detailed insight into existing research patterns, gaps, and uncovered areas of the field.

A. METADATA ANALYSIS

We start our quantitative analysis by presenting in Fig. 2 the time distribution of the selected publications. As expected, the interest in the topic has been increasing constantly in the considered time frame, as proven by the trend of the number of publications since 2015.

1) PUBLICATION OUTLETS

For the quantitative analysis, we considered the metadata of the selected papers, thus performing a preliminary classification. In Fig.2 the temporal distribution of the publications is shown: as we argued, there is an increasing trend in the number of papers over the years; this is certainly a consequence of the growing interest in SDN security both from the

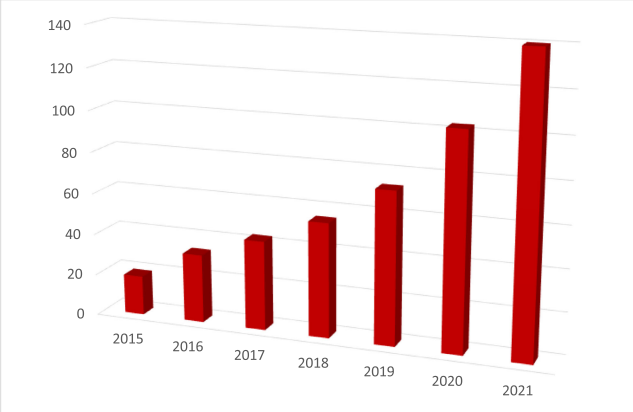


FIGURE 2. Paper distribution by year.

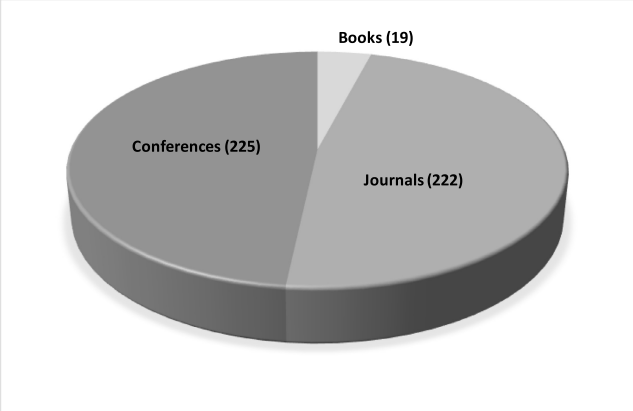


FIGURE 3. Paper distribution by type of publication.

academic and industrial worlds [ds303], [ds416]. A classification by publication category follows, in Fig. 3. As expected in the final data set we found also several reviews and surveys, 44 papers precisely, that satisfied our requirements described in III.

We continued with a classification by publication site, depicted in Fig. 4. The names of the conferences and journals are shown in the graph with their official acronym, if available. With reference to the conferences, it can be derived that there is a relatively uniform distribution among the various publication sites; this is not so true for journals, where there is a predominance of CN and IEEE Access, followed by NCA and IJCS with lower frequency (see App. VIII-B for the acronyms).

B. QUALITATIVE RESULTS

In this section, we make considerations derived by reading the selected papers and evaluating them in the light of the research questions, presented in Section IV.

1) THREAT MODEL

From the combined result of questions Q1 and Q4, we can derive that the papers that use threat models are 17% of the total. Among these, only 7 adopt the standard STRIDE model. In addition, there are 12 papers that, even if they do not use it, mention STRIDE in relation to existing literature.

STRIDE is used on surveys that aim to carry out wide-ranging studies on the safety of SDN; these papers do not focus on a single attack, rather aiming to classify and evaluate sets of attack [ds15], [ds34], [ds383]. In 3 papers, STRIDE is mentioned in connection with monitoring and measurement tools [ds76], [ds92], [ds141]. An important thing worthy of notice is that most of these papers that explicitly use STRIDE are 2015 and 2016 papers, which indicates that, however still considered, threat analysis is moving to a new evolution of Threat models, especially for SDN environment.

Without explicitly mentioning the STRIDE threat model, there are 302 publications - 64% of the total - that satisfy question Q2 and therefore deal with these aspects. A graphical representation of the distribution of the attacks considered in the papers is provided in Fig. 5. As can be easily seen from the graph, the papers tend to deal with Denial of Service attacks and their related aspects; the remaining attacks, namely Spoofing, Tampering, Repudiation, Information Disclosure, Authentication, and Authorization, are widely present in the literature, albeit to a lesser extent. Finally, only 7 papers deal with aspects related to the Elevation of Privilege, one of which [ds15], however, uses the STRIDE threat model.

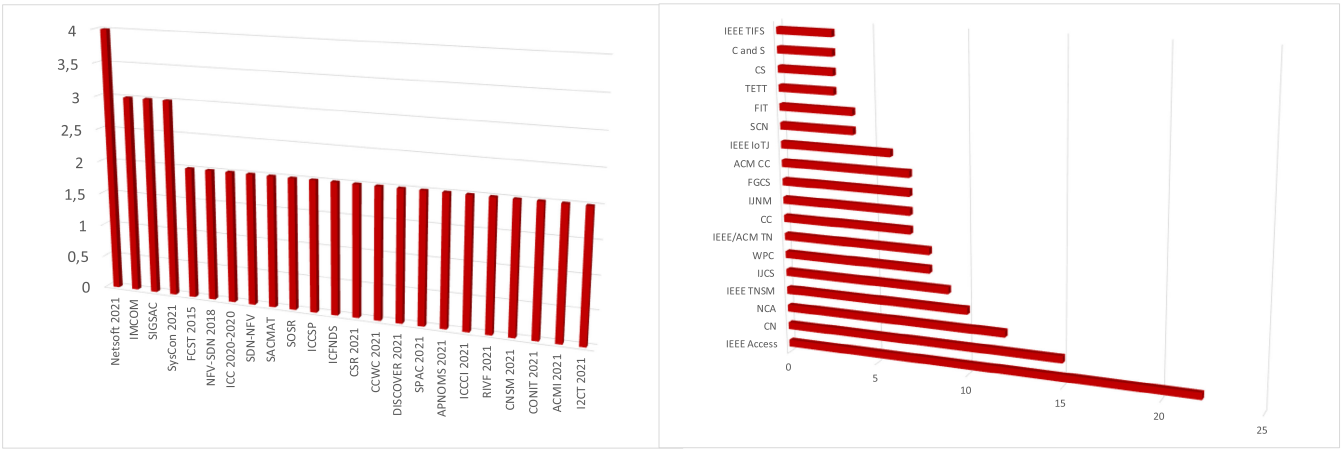
Apparently, the PASTA threat model is never mentioned, let alone adopted. It is therefore possible to state that the most widespread trend is the use of custom threat models, formulated *ex novo*, except in rare cases [ds260], [ds336], [ds404], [ds419]. The custom threat models are mostly aimed at mitigating specific attacks - of a very heterogeneous nature - and are totally tied to that specific threat, making it impossible to generalize them.

Furthermore, threat models are used extensively in connection with DoS/DDoS attacks. These classes of attacks are made up of numerous execution modes, each exploiting a particular vulnerability; the threat models formulated for DoS/DDoS cover in detail a single attack scenario. We argue that there is a lack of a common structure in the threat models, which can form a basis for developing specific models for the different DoS/DDoS attacks.

In conclusion, the analysis did not reveal the predominance of any standard formalism for threat models; this is certainly due to the complexity of the SDN architecture and to a large extent the trend to use SDN in relation to Denial of Service attacks (see Section V-B4).

Insights

Fragmentation of outlets: There are no reference venues for the area of SDN security. This makes it difficult for researchers and practitioners to keep up with the state of the art, as well as to find dedicated conventions where they can discuss this topic with the rest of the community. This is particularly evident with conferences, while we can identify 4 to 5 journals that collect most of the references.



(a) Conferences (b) Journals

FIGURE 4. Paper distribution according to publications site (the acronyms refers to major journal and conferences and are explained in the Appendix).

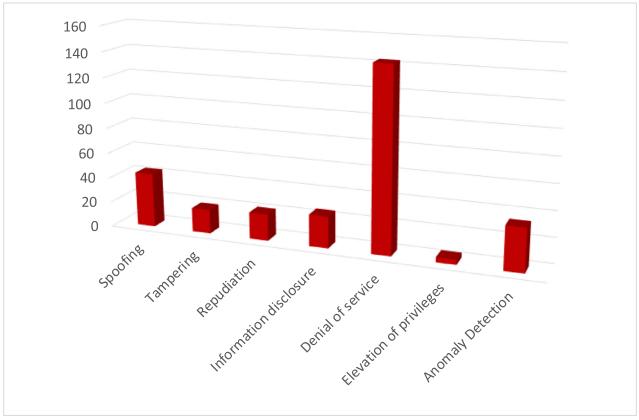


FIGURE 5. Paper classification based on attack type.

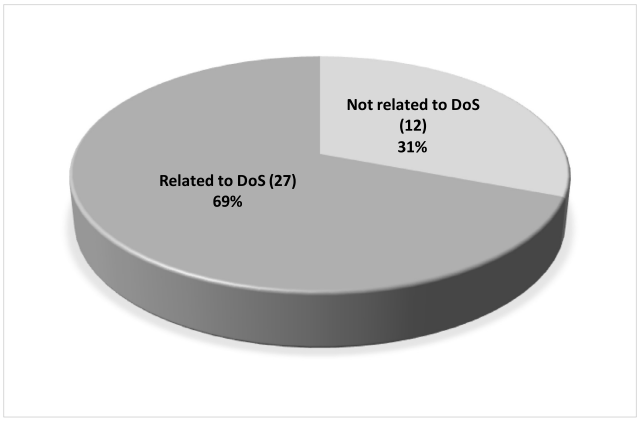


FIGURE 6. IDS/IPS distribution according to the denial of service attacks.

2) SECURITY STRATEGY/APPROACH

From questions Q6 and Q7 we can see that 37 papers mention SDN solutions that rely on IDS functionality, thus accounting for 8% of the total of the articles. Furthermore, 17 papers that mention IPS, 4% of the total. Overall, 54 articles talk about IDS or IPS (Q6 OR Q7).

As in the previous section, there are many differences in the implementation, the proposed architectures, and on the objective of the work. An overview of the collected data can be found below:

- Several papers, such as [ds22], [ds61], [ds234], [ds367] propose IDS functionalities implemented at the SDN controller level, in a case in particular [ds398], deployed in the cloud. Furthermore, others propose controller-level implementations of Ryu (sometimes in connection with the Snort software) [ds50], [ds109], [ds389]. Generally, there is a close and growing relationship between intrusion detection and the use of Machine Learning techniques such as [ds178];
- The works [ds246], [ds260], [ds313], [ds442] implement at application level some sort of IDS/IPS service;
- [ds392] features an IDS architecture integrated into an OpenFlow switch, resulting in an Anomaly Detection Rate of 91.98% and a false positive detection rate of 0.55%, considering multiple attacks;
- [ds6], [ds25], [ds195] instead propose more complex systems, structured and implemented on multiple levels of the SDN;
- [ds136] and [ds346] just propose the study of sampling methods for IDS;
- [ds388] implement a Collaborative IDS, external to an SDN network, based on Snort for intrusion detection and on blockchain to protect the transmitted data, capable of detecting different types of attacks and with particular pay attention to the insider threats to which the collaborative model is exposed. Blockchain-based verification for IDS seems to be a new growing trend in the fields, with interesting applications shown in [ds211], [ds239].

Insights

Dedicated attack trees and threat models: While there are attacks that specifically choose SDN for both the offensive and defensive approach, such as those that leverage the scalability of SDN architectures to cause a denial of service, there are no dedicated threat models to help developers become aware of those particular threats.

Insights

Global view/control: The centralized nature of the SDN controller introduces the need for technologies that provide global yet decentralized observability and control, i.e., tools that aid in the enforcement of security policies over a whole architecture without single points of failure.
Reaction & recovery techniques: while we found solutions to prevent and detect attacks, there are only a few proposals of SDN-based active defense systems that could react to and recover from them.
Comprehensive technological references: SDN use diverse sets of technology stacks, each characterized by peculiar exploits. To secure such architectures effectively, system administrators need dedicated technological references to avoid known threats.

It should also be noted - as shown in Fig. 6 - that more than half of the papers that satisfy Q6 or Q7 are strictly related to the defense of Denial of Service attacks, further confirming the predominance of the latter area in the literature. There is hardly any mention of Threat Intelligence (Q8, 3 paper); Exfiltration Leak (Q9) and Insider Threat (Q10) are dealt with to a greater, but still limited extent, for a total of 25 papers.

3) INFRASTRUCTURE

The adoption of the NFV paradigm is a natural complement to SDN that allows obtaining a completely virtualized network architecture and facilitates the monitoring and management of the network. There is a medium-low presence (of about 12%) of works that exploit NFV (Q11) in the dataset. The trend is therefore to consider the SDN architecture standalone, considering only threats and security vulnerabilities that concern SDN *per se*. However, some papers present software implementations on NFV, which demonstrate how network orchestration can assist the security of SDN. For example, [ds277] exploits NFV to implement a *Data Plane* monitoring system based on Machine Learning techniques to detect botnet attacks. Reference [ds155] presents a *closed-loop* system, where NFV monitors traffic to detect DDoS attacks and alerts the SDN controllers whenever an attack is spotted, in order to adopt mitigation measures. In [ds194] otherwise, authors proposed a monitoring and security framework for multi-access edge computing infrastructure based

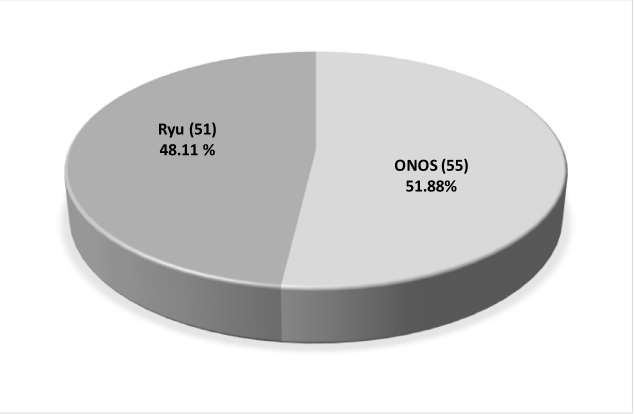


FIGURE 7. ONOS and Ryu mentions.

on the deployment of NFV over an SDN architecture. NFV certainly takes on more relevance when it is used in more structured areas, such as Cloud computing or 5G. In fact, the following contributions can be highlighted:

- [ds438] proposes a security framework for 5G, based on SDN/NFV;
- [ds121] implements two VNFs and an SDN application, in order to detect and mitigate botnet attacks in 5G;
- [ds6] presents an IDS/IPS, based on SDN/NFV and designed for the protection of 5G networks.
- [ds456] presents a service function chain deployment in cloud-fog computing networks

We then tried to understand if there are common ways of orchestrating or managing NFV architectures, for instance, adopting the ETSI NFV-MANO approach, and maybe exploiting the open-source implementation Open Source Mano (OSM) made available by ETSI. Following a targeted check, in connection with question Q12, it appears that in the analyzed papers there is no mention, let alone of the adoption, of OSM. Our feeling is that the management and orchestration of the virtualized network infrastructure are not considered relevant in the literature we have analyzed.

In this group of questions, we also evaluated the number of publications that mention or are based on known open-source implementations of SDN-related building blocks, such as Mininet for network emulation or Onos and Ryu as controller implementations. A medium-high number of publications - 180, equal to the 38% of the total - mention at least one of these technologies.

Onos and Ryu are widely mentioned in relation to IDS/IPS or simple threat detection mechanisms (see section V-B2). In Fig. 7 we show the distribution of the mention of Onos and Ryu in the papers that satisfy Q12. Regarding this, we highlight a survey that aims at fully analyzing the security of SDN controllers comparing the main open-source implementations.[2] In this work, 9 principles are suggested and

[2]OpenDaylight (Lithium), ONOS (Junco), Ryu (3.5), Floodlight (1.2), OpenContrail (R4.0).

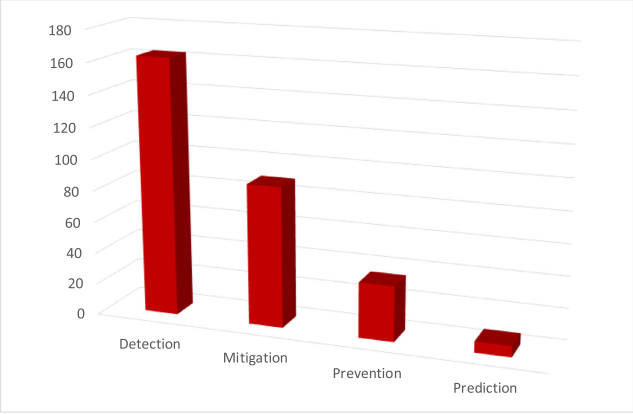


FIGURE 8. Machine learning usage in DoS detection and mitigation.

explained as a methodology to safeguard an SDN controller [ds383].

Dixit et al. [ds101] identify vulnerabilities in infrastructures that use NMDA[3] and show their impact and risk on the availability, integrity, and confidentiality of an SDN network.

The P4 language usage is very scarce in the literature considered. Noteworthy contributions are [ds440] that proposes,[4] a new architecture for packet parsing, integrated into SDN switches and strongly based on the P4 language specification and on the security *by design* offered by Blockchain, and [ds466] where authors propose a packet forwarding control mechanism based on P4 for software-defined networking.

Finally, the use of the Mininet network simulator is very widespread: 160 papers out of the 180 that satisfy Q12 mention this software. Mininet seems to be very effective and widely used for simulation and evaluation purposes of the research carried out.

About one-third of the considered papers adopt or mention Machine Learning techniques and algorithms (Q13). There is a strong correlation between Machine Learning and IDS/IPS systems, as seen in sect. V-B2. While not implementing real IDS/IPS, there is a large number of papers dealing with the detection and mitigation of attacks, mainly Denial of Service. Here too there is an evident influence of the Machine Learning world. Further considerations in this regard are provided in the next section.

Insights

SDN solutions are built around commercial technologies: Commercial controllers such as Onos and Ryu are widely used. NFV is mostly used as a supporting technology to the SDN while Mininet is by far the most used software to simulate the use cases. Most of the papers considered adopting a traditional SDN approach to the infrastructure since the P4 language is usually not the first option.

[3]Network Management Datastore Architecture.
[4]Blockchain-enabled Packet Parser.

4) MAIN GOAL

In this subsection, we continue discussing the information obtained regarding the general main purpose that can be inferred from the dataset. By briefly examining the data, it is clear that the absolute majority of the works aim to protect against Denial Of Service attacks (Derived from Q14). In fact, 186 papers - 39% of the total - propose strategies to detect, mitigate, prevent, or predict the attacks in question. Furthermore, as anticipated in Section V-B1, we can count a total of 231 papers (50%), if we also consider papers that do not deal exclusively with DoS. Fig. 8 shows the distribution of contributions by defense method implemented: we find the highest frequency in detection and mitigation strategies, often implemented jointly. There are also contributions related to methods of prevention and prediction, albeit to a lesser extent; these usually have to do with the implementation of real IPS: for example, in [ds109] an IPS that includes a Honeynet is proposed, in [ds398] otherwisethe IPS is an NFV that can be deployed into the cloud. SDN has in fact been also used to perform deep packet inspections, as proposed in [14].

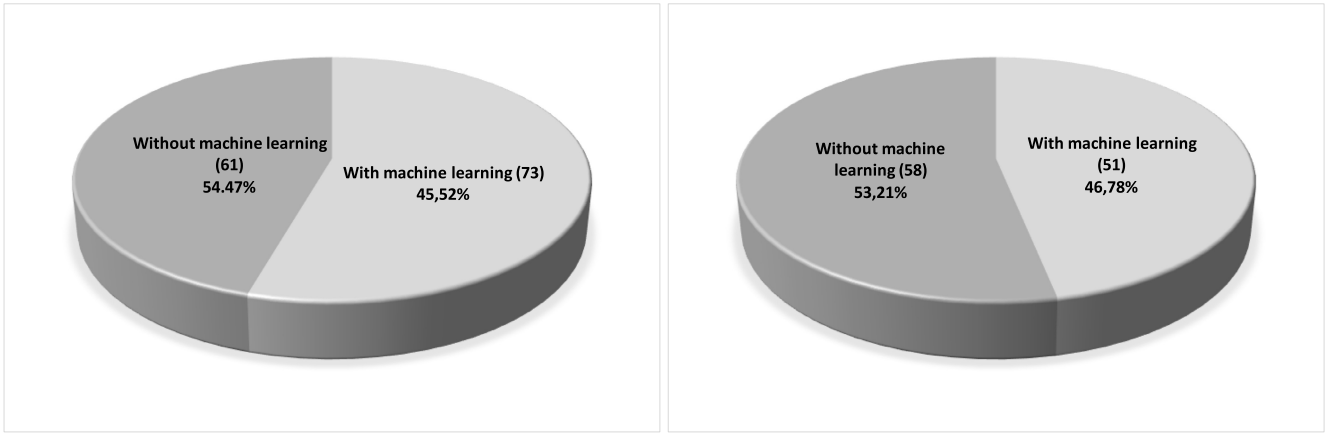
Recalling the detection and mitigation methods, in Fig. 9 it is possible to see how both are strongly linked to algorithms or Machine Learning techniques; therefore, a good rate of effectiveness is shown in the use of Machine Learning to tackle DoS.

With regard to industrial network environments, there is a low number of contributions (derived from Q14). However, some of the 8 papers that meet these requirements are noteworthy. For example, [ds283] proposes a reactive security mechanism based on SDN/NFV to monitor industrial networks, in which there is also a honeynet. Similarly, [ds315] aims to protect ICS by providing policies for monitoring, detecting, and re-configuring networks via SDN/NFV.

Regarding the mitigation of non-DoS attacks (derived from Q14), there are some articles - in total 15 - dealing with port scanning and spoofing (IP/ARP). These attacks are mostly mentioned in conjunction with DoS, in the context of the IDS/IPS systems described above.

There are also a small number of articles dealing with particular attacks, not related to DoS, to which SDN is vulnerable. The most interesting are:

- In [ds428] the network isolation attack is discussed, which allows an attacker to access user network privileges without being aware of this. An implementation based on ONOS is proposed, in order to prevent this attack and other spoofing attacks;
- Zhao et al. [ds459] highlight the problems deriving from the link discovery process of SDN networks, proposing a new operational scheme. The experimental evaluation shows that this scheme is able to solve link fabrication problems;
- [ds151] extends the study of the aforementioned problem, discussing topology poisoning attacks by proposing a topology verification scheme to prevent host hijacking and link fabrication attacks.



(a) Detection (b) Mitigation

FIGURE 9. Machine Learning usage distribution for DoS Detection and Mitigation.

- [ds42] deals with DDoS but the solution, in this case, is to protect the SDN controller itself.

Insights

Denial of Service-oriented research: The most common objectives of the papers are mitigation, detection, and prediction of Denial of Service attacks. The papers usually do not deal with industrial topics or attacks different from DoS.

5) MACHINE LEARNING USAGE

A well-defined trend in the dataset is the use of Machine Learning techniques within SDN solutions. The first works appear as early as 2015 but over time the use of ML algorithms to support SDN security analysis has become an increasingly common solution. We also find this trend in our dataset where 163 papers (about 34% of the total) consider Machine Learning techniques and algorithms. The techniques used are different, ranging from Random Forest classification to the most common Bayesian statistics up to reinforcement learning techniques. One pattern, however, is quite clear and sharp. Most of the papers use Machine Learning on DoS attacks. Since it was impractical to describe all 163 papers, we have prepared Table 2, which groups them by category and type of Machine Learning technique, describing those that we consider relevant.

Most of the papers deal with classic DoS, more precisely DDoS. The main purpose of the majority of the works is, of course, to identify and mitigate an attack in progress. Most of these jobs, therefore, try to replace an IDS or create rules for the same IDS to which they link. In works such as [ds45], [ds365], [ds391] for example, authors evaluate several Support Vector Machines (SVM) techniques to detect abnormal behaviors and attacks as early as possible. An important research branch uses Machine Learning directly on the controller, to try to defend or mitigate the effects of a DoS attack. The centralized nature of SDN controllers, in particular, is a topic that this context has been widely discussed.

For example, in [ds253] the authors proposed a Supervised Learning Approach to Mitigate Host location Hijacking Attacks, implemented in the SDN controller. This plugin controller monitors the legitimacy of the hosts and identifies users impersonating the hosts in the data plane, and can be deployed in both centralized and decentralized SDN controller setups.

In [ds349] a new full architecture is otherwise proposed, spanning the stack from the data plane to the application level, able to both identify DoS attacks and trigger events to mitigate them at every level of the architecture.

A similar strategy has been used in [ds256], where the authors proposed a microservice-based controller architecture that is able to efficiently scale horizontally in case of a DoS attack.

In [ds3] otherwise, authors identify five control functions required by a realistic production network to accomplish essential network services, and then they analyze threats and defense mechanisms pertaining to these five functions when implemented by L2 networks. A new evaluation framework to objectively compare the security of both network paradigms is provided, using two threat models.

In [ds445] the DDoS detection is based on an entropy detection scheme, which is implemented in conjunction with its respective ISP domain. Another very interesting Machine Learning DDoS detection mechanism can be found in [ds250]. In this case, the authors exploit the features of a programmable data plane in P4 language. A very similar approach has been made in [ds38] where in this case authors proposed a ML classifiers for the mitigation phase, based on five threat vectors that represent compromised controllers.

There are also several works that aim at bringing ML capabilities inside the controller for specific DoS attack vectors. A good example is [ds181], where authors analyzed three supervised classifiers and four semi-supervised classifiers for

five types of saturation attacks (TCP-SYN, UDP, ICMP, IP-Spoofing, and TCP-SARFU) and their combinations, through a detection framework which uses controller monitoring data such as CPU utilization, channel bandwidth, and flow table utilization.

Another important trend that we have found is deep/reinforcement learning, which leverages one of the strengths of SDN. We noticed that this ML technique is widely adopted to identify anomaly behavior (especially DoS). The main reason for this choice is that it exploits the reconfiguration capabilities of the SDN architectures which allows real-time generation of aggregated data. Reinforcement learning exploits these features by feeding algorithms with new rewards.

For example in [ds189] authors propose a non-intrusive traffic sampling mechanism for multiple traffic analyzers on an SDN-capable network using a deep deterministic policy gradient, which is a representative deep reinforcement learning algorithm for continuous action control.

In [ds353] a framework is developed, with a deep learning Boltzmann machine-based flow analyzer to identify the anomalous switch requests. This framework is then integrated with a blockchain mechanism in which all the switches are registered, verified (using zero-knowledge proof), and, thereafter, validated in the blockchain using a voting-based consensus mechanism.

Previous works used Deep Learning in order to strengthen the mitigation mechanism for large-size attacks. But there are also several works that use Deep Learning to improve the detection phase. A good example is presented here in [ds407] where a DDoS attack detection method based on information entropy and deep learning is proposed. Primarily, suspicious traffic is inspected through information entropy detection by the controller. Then, fine-grained packet-based detection is executed by the convolutional neural network model to distinguish between normal traffic and attack traffic.

A recent alternative approach is presented in [ds105] where a new deep learning algorithm, denoted the Parallel Online Deep Learning algorithm, is defined in order to update weights on the fly according to both aforementioned constraints simultaneously. A weight defines the amount of data allowed which can be transmitted by a node and that is dynamically updated according to its contribution to the queuing capacity of the controller, and the number of flow rules in the switch. In [ds190] otherwise, authors proposed a feature dynamic deep learning approach for DDoS mitigation within the ISP domain

Deep Neural Networks are also used in conjunction with an IDS in an SDN network, such as in [ds387] where, for the purpose of effective attack detection in a test-bed, a flow-based anomaly detection is deployed with Deep Neural Networks to improve the signature-based IDS limitation with a higher detection rate and low false-positive triggers.

There are also several hybrid approaches that combine a Deep Learning algorithm in support of a well-known one for better long predictions. For example, in [ds227] a hybrid Cuda-enabled DL-driven architecture is proposed, which leverages the predictive power of Long short-term memory and Convolutional Neural Networks for efficient and timely detection of multi-vector threats and attacks.

Another interesting trend in Machine Learning is its vertical usage over a specific category of DoS, namely Low-rate DoS (LDoS) attacks. Machine Learning has been proven to be very effective for this kind of attack. A good example of this approach can be found in [ds462] where to improve the detection accuracy of the low-rate DDoS attack against the SDN data layer, a new method based on Factorization Machine is proposed. The features extracted from the flow rules are used to detect low-rate DDoS attacks, and the detection of low-rate DDoS attacks based on Machine Learning algorithms is implemented.

Similar work has been made in [ds312] where authors, taking advantage of flow based nature of SDN, proposed a Generalized Entropy (GE) based metric to detect the low rate DDoS attack to the control layer. In [ds372] otherwise, also the mitigation steps after detection are introduced, with a framework based on the histogram-based gradient boosting and finding peaks algorithm to detect LDoS attacks and mitigate their influence in the SDN in real-time. In [ds66] the machine learning algorithm is otherwise used to choose the target in the moving target defense scenarios. Considering a specific LDoS attack against port (Portscan), interesting work is [ds267], where a detection and mitigation system of DDoS and Portscan attacks in SDN environments (LSTM-FUZZY) is presented.

One of the most relevant trends for Machine Learning applied to the security of SDN is the adversarial attack/behavior. Adversarial Machine Learning is a Machine Learning technique that attempts to exploit models by taking advantage of obtainable model information and using it to create malicious attacks. In the last year of the collected dataset, we noticed an increased interest in this field with applications to analyzing such attacks both from an offensive point of view (generating them) and a defensive point of view (detecting them). A good (offensive) example can be found in [ds17] where, in order to investigate Adversarial Attacks in SDNs authors implemented an anomaly-based NIDS, Neptune, as a target platform that utilizes a number of different Machine Learning classifiers and traffic flow features. Then an adversarial test tool, Hydra, has been developed, to evaluate the impact of adversarial evasion classifier attacks against Neptune with the goal of lowering the detection rate of malicious network traffic.

From the defensive side, two interesting work exists. One can be found in [ds268], where three adversarial training procedures to improve the detection performance of a framework concerning adversarial attacks are proposed. The designed framework detects flooding DDoS attacks based on DL for SDN environments. The second one is otherwise [ds203] where authors use adversarial techniques for the availability

and reliability analysis of cloud computing under economic denial of sustainability (EDoS) attack

Insights

Machine Learning Trend:
There is a strong and clear trend indicating SDN as an enabling and supporting technology for the development of Machine Learning based solutions. Obviously, the application for the detection phase covers the majority of the works, but in recent years interesting trends are becoming increasingly popular such as:

- **Reinforcement Learning** which takes advantage of the ability of SDN networks to reconfigure in a very simple and fast way.
- **Adversarial Behavior** that uses SDN to simulate attacks that can test the robustness of rule-based IDS systems.

6) DoS CLASSIFICATION

The absolute majority of the dataset, as pointed out in V-B4, deals with the Denial of Service attacks. This attack aims at making services unavailable to the intended users by saturating the resources. Usually, these kinds of attacks flood the target with traffic to trigger crashes. Authors in [ds266] propose a solution to counter the flow table attack by adjusting hard and idle timeouts to reduce the number of flow rules. Using packet count, this solution adequately adapts the number of flow rules under a DoS attack. In [ds176] a security SDN solution against DDoS, man-in-the-middle, spoofing/masquerading attacks for IoT is shown. The environment was tested using ONOS. Work in [ds251] proposes a Kerberos-based authentication solution to verify the sanity of new hosts joining an SDN. This solution was designed to counteract controller and host impersonation attacks. Another interesting solution can be retrieved in [ds324] regarding an IDS-like solution to detect attacks in an SDN network using online clustering. This solution was evaluated with 48 databases attacked by DDoS and portscans, obtaining DDoS detection in a relatively short time in every scenario.

In [ds447] a flow message linear analysis model able to effectively detect malicious SDN switches in the Tactile Internet is proposed. It analyses attacks such as controller exhaustion attacks, flow table exhaustion attacks, and flow redirection attacks. In [ds296] indeed authors designed a scalable intrusion detection and prevention system (IDPS) to prevent large-scale SYN-flood attacks in an SDN environment. In [ds328] otherwise a point detector IDS to monitor performance metrics to detect DDoS attacks using constraint programming in software-defined wireless sensor networks (SDWSN) is introduced. In [ds269] authors developed a DDoS attack detection and mitigation system that uses a random forest Machine Learning algorithm. The solution was tested on a Mininet-Ryu testbed using Openflow. Finally, in [ds99] authors proposed a big data framework to contrast processing limitations during large-scale SDN networks DDoS attack, work that has been similarly proposed in [ds179] where the framework deploys a multi-agent autonomous system. Most of the works exploit a large number of external technologies like Machine Learning, NFV, Blockchain, and Convolutional Neural Networks. The literature is overall very scattered in terms of targets and environments considered.

Moreover, the literature strongly concentrates on different flavors of DoS attacks. For example, LDoS is a typology of Denial of Service that aims to intentionally degrade the quality of TCP links by throttling TCP flows to a small fraction of its ideal rate with a periodic small pulse sequence. Work such [ds212] analyzes LDoS attacks by proposing an attack detection system based on Bat Algorithm and BP Neural Network. In [ds418], on the other hand, authors analyzed Slow HTTP DoS (SHD) attacks, the flavor of LDoS that targets web servers. This solution adopts a credibility-based countermeasure against SHD attacks. In [ds373] author proposed a real-time framework to detect LDoS attacks in SDN, named Performance and Features (P&F), which uses Machine Learning. This type of DoS attack is hard to detect since it is effectively hidden in normal traffic and it does not produce a noticeable outcome such as service unavailability.

Another DoS trend in literature is detecting and mitigating Economic Denial of Service (EDoS), an attack that aims to scale up the pay-per-use resource usage to make the cloud user pay an unexpected amount. In [ds100], for example, the authors presented a Neural Networks-based scheme that produces anomaly scores by learning a multivariate attribute. In [ds333] on the other hand, a model to mitigate TCP SYN flooding-based EDoS attacks is implemented. In [ds203] authors proposed a semi-Markov approach aimed to evaluate the availability and reliability of cloud computing under an economic denial of sustainability attack. This kind of attack is very different from traditional DoS since it only focuses on generally producing an economic loss to the target. Moreover, we argue that these kinds of attacks should be studied by also analyzing the carbon footprint they imply.

Moreover, the dataset shows that the scientific community is increasingly focusing on different flavors of DoS, such as LDoS and EDoS. We claim that these new kinds of attacks can be an interesting topic of study for SDN in the future. Another very important task that literature generally poses is to enhance the explainability of these attacks by exploiting the SDN paradigm, by being able to track down the source of DoS attacks, and then develop more fine-grained mitigation solutions and policies to punctually counteract these threats.

TABLE 2. ML-based classification of the paper of the dataset.

ML Technique	Generic DDoS	LDoS	Adversarial Attack
Generic Machine Learning	[ds7], [ds391], [ds45], [ds262], [ds90], [ds182], [ds70], [ds317], [ds364], [ds252], [ds338], [ds115], [ds49], [ds215], [ds302], [ds309], [ds245], [ds295], [ds436], [ds383], [ds322], [ds221], [ds150], [ds103], [ds291], [ds27], [ds116], [ds435], [ds132], [ds135], [ds134], [ds127], [ds380], [ds109], [ds242], [ds171], [ds250]	[ds14], [ds321], [ds128], [ds417], [ds437], [ds155], [ds445], [ds259], [ds327]	[ds253], [ds8], [ds218] [ds62], [ds17], [ds378]
Deep Learning	[ds407], [ds205], [ds227], [ds208], [ds389], [ds16], [ds350], [ds189], [ds450], [ds217], [ds427], [ds288], [ds458], [ds86], [ds348], [ds190], [ds422]	[ds384], [ds353], [ds238], [ds365], [ds105], [ds387], [ds434]	[ds268]
Reinforcement Learning	[ds189], [ds90]	[ds189]	[ds156], [ds444]

Insights

Flavours of Denial of Service: the rise of new flavors of Denial of Service attacks considered in literature outlines new challenges for the scientific community. LDoS and EDoS change the paradigm of tackling DoS attacks, making SDN a useful paradigm to mitigate them.

7) BLOCKCHAIN USAGE IN PROGRAMMABLE NETWORKS

Blockchains [8] and, more broadly, Distributed Ledger Technologies are one of the most trending topics of the last years [10]. In thecontext of network programmability, the main applications of Blockchain-related technologies are related to SDN security [ds263]. The main contribution of Blockchain technologies applied to SDN can be found in [ds263]. As stated in this work, the main solutions exploit the immutable state of the Blockchain to create authentication layers or to increase the overall reliability of the network. One of the adopted solutions is to enforce security policies in the distributed ledger [ds340].

Aside from works described in [ds263], we describe the most popular approaches observed in the dataset. The straightforward application of Blockchains, tied to the design of this technology, is the possibility to build Authentication-Authorization-Accounting (AAA) systems. One of the main examples of this approach can be seen in [ds141], in which the authors propose a system that manages the AAA proprieties through a Blockchain to achieve immutability of the database and native decentralization. This is similar to the work proposed by [ds72], where the authors describe an authentication process, verifiable through the data saved in a Blockchain. In [ds199], the ledger is used to authenticate an IP address that originates traffic. Using this approach, DDoS protection can be easily built. A theme related to AAA is the monitoring of the infrastructure, this feature can be easily certified by a Blockchain. This is the approach employed by [ds399], which verifies the probe's data and commits them using a distributed ledger.

Blockchains can be used to create *collaborative networks*. References [ds112], [ds240], [ds353], [ds388] create networks of this kind to set up a collaborative intrusion detection system, in which the Blockchain is used to build trust in collaboration. Using this kind of setup, the network could be created in a secure way, without rogue intrusion detection and prevention systems.

The Blockchains can be used with protected models to avoid a problem called *Model Poisoning*. This problem can arise using a detection system based on a model trained over a dataset if the dataset gets *poisoned* - e.g. some rogue values get injected with a specific label - the system can be manipulated in order to be controllable by the attacker. As described in [ds29], Blockchain technologies can be used to validate the model and make this attack unfeasible. While being totally transparent by design, the work described in [ds29] protects a model distributed as an Intellectual Propriety, without making proprietary information available to every user. Another interesting path we can identify is represented by the usage of the blockchain throughout machine learning techniques, in order to verify the reputation of a node for several goals, as showcased in [ds171] for crypto miners.

This kind of technology can be integrated into the SDN internal workflow. For instance, [ds5] employs a distributed verifiable ledger to filter and maintain a secure flow database. In this same field deserves to be mentioned the work in [ds239] which is one of few works of this dataset that addresses the insider threat problem, enhancing a challenge-based collaborative intrusion detection network against insider attacks using blockchain. The last technology presented is the integration of the Blockchain in the data plane parsing procedure itself. This strategy is implemented by [ds440]. This work leverages the features of P4 language and blockchain to implement trackable and inspectable policies,

securing that the data plane parser will implement policies certified by the Blockchain.

In Table 3 we summarize the main classes of contributions in the field of Blockchain and network programmability.

Insights

Distributed Ledgers: The adoption of distributed ledgers and Blockchains can undoubtedly help the security of SDN and Programmable data plane ecosystem in various fields. Certified models and monitoring are performed using a so-called Blockchain layer. Whereas most publications are focused on Security, works on performances are present in literature.

8) TECHNOLOGY POPULARITY

A number of different technologies are employed in research activities regarding programmable data planes and Software Defined Networks. These technologies can be divided into research tools and business-related infrastructures and protocols.

One of the most notable examples is the ubiquitous[5] adoption of mininet.[6] This tool is mainly used to generate realistic network topologies, making the experiments reproducible and easy to configure thanks to Python programming language. Python plays a central role in the ease of use, as stated by the literature. Another example of this is the Ryu controller (present in 29 works in our dataset including [ds228], [ds343]). This controller is written in Python and implements themost common switch behaviors. A different controller, which implements also practical web interfaces is ONOS [3]. This controller can be considered easier to configure than Ryu, but a little more cumbersome to extend, due to its core language: Java.[7]

New network programmability paradigms such as P4 or 5g-related technologies (e.g. MEC) are trending in the Network programmability scenario. These technologies, when compared to older technologies such as SDN and containers are still not on the same level of popularity (10 references for P4 and a single reference for the 5g MEC). The possibility offered by these technologies as enablers is the main point of adoption in academic research.

Insights

Technology trends: The flexibility offered by new paradigms is getting more and more traction in the network programmability research field. Ease of use and programming is, probably, one of the main factors that favor the adoption of tools such as mininet or Ryu.

[5]In the dataset there are 62 works that use or refer to mininet, for instance: [ds56], [ds157], [ds175], [ds210], [ds228], [ds233], [ds341], [ds343], [ds360], [ds372], [ds373], [ds378].

[6]http://mininet.org/

[7]https://pypl.github.io/PYPL.html

VI. CONCEPT AND CROSS-CORRELATIONS

In this section, we close our analysis with other two relevant evaluations. First, we created and discussed a keyword text analysis in order to discover any other potential interesting trend. Second, in order to validate the results of our research questions analysis we provide a correlation analysis of the questions, with a quantitative look over the relationships between them.

We conclude with a discussion of potential threats to validity, aimed at preventing bias issues in our methodology.

A. WORD NET CLOUD

The first correlation analysis provides a graphical representation of the most used keywords in the abstract of the contributions in our dataset. To conduct our analysis, we used VOSviewer by [26], a software that offers text mining functionalities for constructing and visualizing co-occurrence networks of important terms extracted from a given corpus. Specifically, we ignored basic words and copyright statements and performed a full count of the words present in the text. We considered only words occurring more than fifteen times, sizing them by their relevance in terms of occurrences. The resulting graph, however, is still too large and complex to convey useful information: for the sake of clarity, we present here a visualization including only the top 75% of most-occurring words.

We report the visualization of the analysis in Fig. 10.

VOSviewer automatically clustered the words in 3 areas using its modularity-based clustering algorithm, which is a variant of the cluster algorithm developed by [4] to detect communities (clusters) in a network that also considers modularity.

We can interpret the clusters as follows:

- The blue (■) area at the top of the figure marks the technical terms of this study, grouping words like *packet* and *layer*. The result is not surprising, since those words describe the building blocks of the domain.
- The green (■) area at the bottom-left corner marks the main terms of the study as *controller* or *attack*. Directly related to the query used to get papers, the results reflect the process as the base of this systematic literature review.
- The red (■) area on the right-hand side identifies properties and application fields, e.g., security, blockchain, and Machine Learning. We find for instance the word *ddos-attack*, as it is mainly cited as a specific property to analyze or protect, rather than a tool to use.

B. CORRELATION BETWEEN RESEARCH QUESTIONS

The amount of data collected in our dataset is large enough to represent a statistically-relevant sample. In this section, we leverage this to study correlations between our research questions, by way of the answers that the publications in our dataset give to each of them. Correlations can be used to understand which of the different aspects of SDN security

TABLE 3. Summary of the analyzed blockchain technologies applied within SDN/Programmable data networks, architecture.

Category	Papers
Authorization or authentication or accountability	[ds141], [ds72], [ds199]
Collaborative Networks	[ds388], [ds112], [ds353], [ds240], [ds239]
Secure Models for IDS or ML	[ds29], [ds171], [ds216]
Secure Monitoring	[ds399]
Security Dataplane-based solutions	[ds5], [ds440]

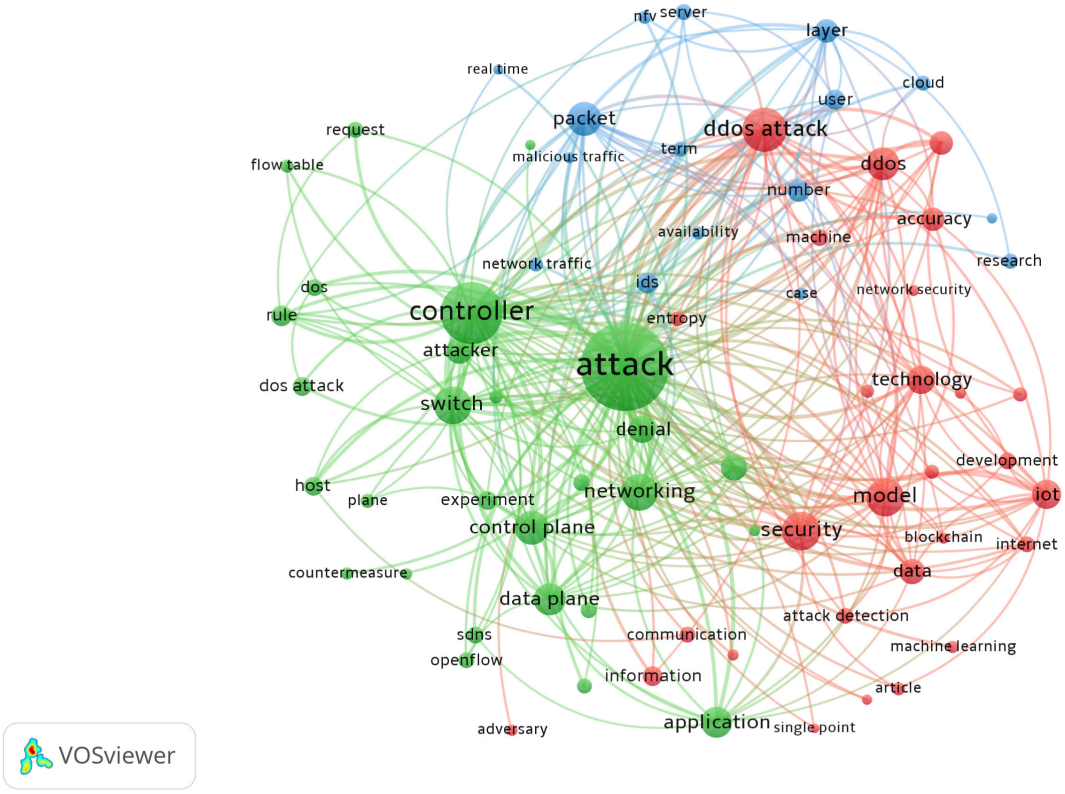


FIGURE 10. Representation of the main keywords found in the abstract of the articles in the dataset. This image was generated with VOS viewer.

offensive or defensive are most commonly in a positive correlation (paired) in the dataset, and which ones are negatively correlated (mutually exclusive).

We report in Table 4 the correlation matrix. While the obtained matrix is symmetric and we could report just one half, in Table 4 we report the full matrix for convenience, to provide a more immediate view of how each question correlates with all of the other ones. We conditionally colored the cells of the Table, first, attributing color intensity according to correlation absolute value—maximal intensity for 100% and degrading towards 0%, second, setting a transition threshold above 23% (absolute value) from blue to orange, to help to spot relevant correlations. Looking at the Table, we notice the predominance of light-colored cells. This result can be interpreted as an indication that the research questions used in this work are mostly orthogonal, and thus suited to cover the reviewed subject with almost no wasteful overlap. In the following, we comment on all positive and negative correlations above/below 23%.

- **Q6-Q7(49.02%):** This strong correlation indicates how IPS and IDS are strictly related. Questions Q6 an Q7 ask if the publication mentions IPS or IDS functionalities respectively. Indeed, in practice, IDS may exist without IPS, but not the opposite, because prevention mechanisms are typically built as a reaction to a detected attack.
- **Q2-Q14(39.34%):** The questions ask if the paper mentions one or more features of STRIDE without mentioning it explicitly and if the paper deals with Denial of Service. The high correlation suggests that a large number of papers treat the topic of Denial of Service since it is the "D" contribution in STRIDE and has Denial of Service as the main goal. Having Denial of Service as the main goal implies that it is a topic of discussion in the paper.
- **Q8-Q10(23.89%):** This "light" correlation maps a link between Threat Intelligence techniques and Insider Threat attacks. If the paper mention/deal with Threat

TABLE 4. Research question correlation table. Color intensity represents correlation absolute value where maximal intensity for 100% and degrading towards 0%, with a transition threshold above 23% (absolute value) from blue to orange, to help to spot relevant correlations.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Q1		5.53%	-11.41%	-6.97%	-4.76%	-7.22%	-4.39%	-1.81%	11.05%	12.96%	-5.25%	-5.58%	-3.96%	-0.02%
Q2	5.53%		8.60%	-10.52%	-7.60%	-18.99%	-21.40%	1.28%	0.14%	-2.02%	3.94%	12.72%	8.30%	39.34%
Q3	-11.41%	8.60%		10.78%	0.22%	-1.26%	-16.77%	5.37%	6.65%	5.26%	-12.34%	11.71%	-9.19%	-10.95%
Q4	-6.97%	-10.52%	10.78%		11.09%	6.05%	3.03%	18.60%	14.75%	21.26%	4.06%	5.25%	-4.92%	-23.45%
Q5	-4.76%	-7.60%	0.22%	11.09%		6.45%	5.24%	-4.76%	-2.85%	1.31%	2.87%	5.21%	-0.28%	-12.60%
Q6	-7.22%	-18.99%	-1.26%	6.05%	6.45%		49.02%	-7.22%	-7.34%	11.64%	14.78%	-13.87%	21.81%	-13.58%
Q7	-4.39%	-21.40%	-16.77%	3.03%	5.24%	49.02%		-4.39%	-3.70%	6.59%	6.50%	-14.76%	9.24%	-8.14%
Q8	-1.81%	1.28%	5.37%	18.60%	-4.76%	-7.22%	-4.39%		20.92%	23.89%	-0.85%	5.78%	-10.16%	-12.70%
Q9	11.05%	0.14%	6.65%	14.75%	-2.85%	-7.34%	-3.70%	20.92%		22.01%	3.20%	4.25%	-7.83%	-15.81%
Q10	12.96%	-2.02%	5.26%	21.26%	1.31%	11.64%	6.59%	23.89%	22.01%		5.61%	2.99%	-8.34%	-21.26%
Q11	-5.25%	3.94%	-12.34%	4.06%	2.87%	14.78%	6.50%	-0.85%	3.20%	5.61%		-12.76%	5.89%	-7.11%
Q12	-5.58%	12.72%	11.71%	5.25%	5.21%	-13.87%	-14.76%	5.78%	4.25%	2.99%	-12.76%		7.56%	-1.51%
Q13	-3.96%	8.30%	-9.19%	-4.92%	-0.28%	21.81%	9.24%	-10.16%	-7.83%	-8.34%	5.89%	7.56%		20.42%
Q14	-0.02%	39.34%	-10.95%	-23.45%	-12.60%	-13.58%	-8.14%	-12.70%	-15.81%	-21.26%	-7.11%	-1.51%	20.42%	

Intelligence then it is likely that it also works on the mitigation or detection of Insider Threat attacks.

- **Q4-Q14(-23.45%):** This anti-correlation is probably the most interesting. In this case, if the article mentions a threat model or even just one of its aspects (Q4) then it does not include any details relating to a specific attack (Q14). This means that in SDN solutions vertical for a specific attack it is very likely that there is no Threat Model consideration, even partially. This could be advocated by the fact that SDN is used as a complementary tool and for this reason, these types of threats do not properly suit a specific attack scenario.

C. THREATS to VALIDITY

Our study is subject to limitations that can be categorized into a construct validity, external validity, internal validity, and reliability following the guidelines of [ds17].

Construct validity "reflects to what extent the operational measures that are studied really represent what the researcher has in mind and what is investigated according to the research questions.". To mitigate a potential misinterpretation and making sure that the constructs discussed in the interview questions are not interpreted differently by the researchers, we adopted various triangulation rounds using online meetings and we designed a set of binary research questions to foster objectivity in answering them.

Another potential risk regards whether we were exhaustive during the data collection, i.e., whether we may have missed any significant publication in our review. This risk cannot be completely mitigated but to minimize this risk we deliberately chose to have simple and broad keywords giving more initial hits that later were further filtered out.

External validity regards the applicability of a set of results in a more general context and is not a concern for this study since we focus on the the intersection of the fields of SDN and security for offensive and defensive solutions without any attempt of generalizing the findings to a broader context. We do not claim that either our qualitative or quantitative findings should also hold for other large fields.

Internal validity is of concern when causal relations are examined when there is a risk that the investigated factor is also affected by a third factor. This thread is not a concern for this study because we presented only correlations between different factors but did not examine causal relations.

Reliability concerns to what extent the data collection and analysis depend on the actual researchers. This risk has been partially mitigated by selecting as many objective criteria as possible for the filtering and by requiring at least a two-people consensus in case of more subjective decisions. In particular, the retrieval of the publications was performed by using search engines. The first results filtering (Step 2, III) was conducted by running a script that uses objective criteria such as counting the number of present keywords and the length of the publication. These automatically computed results were double-checked by at least two authors to prevent problems due to the parsing of PDFs and to make sure that the language of the publication was English. The second filtering (Step 3,

III) performed by reading the title, abstract, and (if needed) the body of the publication, was performed in parallel by two authors. Decision conflicts were solved by discussion involving at least two authors until a consensus was reached. For the publication analysis (Step 4, III), due to the binary nature and formulation of the questions, the 14 research questions were answered by the author assigned to the publication. To detect possible observer bias and errors, we selected a random subset of 20 papers and had a different author answer the research questions. The calculation of the kappa index of agreement as proposed in [ds5] over the two result sets yielded a value of $\kappa = 0.99996$, giving us statistical confidence over the perceived precision of questions and objectiveness of answers. The reliability of the study is strengthened by being open and explicit about the process of data collection and analysis. For transparency, reproducibility, and reuse, we report the data used in this study at https://doi.org/10.5281/zenodo.6959369, which includes both the final dataset with the answers to all the research questions and also the set of rejected publications.

VII. OPEN CHALLENGES AND FUTURE WORKS

In this section, we draw a summary of the main open challenges that emerged from our study, which forms a call for action for the community of researchers and practitioners working in the field of SDN security and its neighboring areas. The insights that we highlighted in the Sections above have been used to frame some final remarks on open issues and possible future research topics.

A. ATTACK OVER SDN ARCHITECTURE

Indeed a clear message stemming from the analysis is the possible vulnerability of the SDN architectural approach. We do not want to argue intrinsic vulnerabilities of SDN architecture which is not the scope of this article but, from our analysis, many defensive solutions for attack mitigation and detection are conceived by exploiting the strengths of the SDN paradigm. For this reason as future works, we claim that, while adopting SDN technologies for defensive purpose, a deep analysis of what challenges SDN itself introduce must be performed. For instance, the SDN controller, even if distributed and equipped with recovery mechanisms, is clearly a target for security threats, as is the communication channel between the controller and the switches. This is inherent in the original idea of SDN. Nonetheless, the current technological trends may provide methods to overcome this weakness.

B. CONTROLLER AWARENESS

Since the SDN controller is often a single point of failure due to its centralized nature, we argue that future works should focus on providing measures to enforce security policies over SDN architectures. To do this, both architecture-aware tools that check the health of the entire SDN system and the use of new technologies such as P4 can help in preventing, detecting, and mitigating attacks.

C. PROGRAMMABLE DATA PLANE

Data plane programmability, for instance, implemented with the P4 language, seems to become the new trend in increasing the strength of SDN defensive solutions. P4 can keep the switches working without the need for a software controller and could provide fine-grained statistics that can be used to perform detailed network traffic analysis, offloading the intelligence from the control plane to the data plane.

D. DEDICATED ATTACK TREES AND THREAT MODELS

Software Defined Networks are subject to a variety of attacks that leverage the architecture to cause threats, in particular denial of service attacks. The literature suggests that there is not a dedicated threat model to help developers to be aware of those threats. This clarifies how security implemented with SDN, even if the paradigm is mature and largely studied, is still not a standard topic. We argue there should be a threat model to help developers to focus on more granulated threat categorization. The effort of building a standard threat model could help the development of security-compliant applications and analyze architectures to attest to their security coverage.

E. ACTIVE DEFENSE AND MITIGATION SOLUTIONS

The vast majority of the literature focuses on attack prevention and detection. There is little to no work that includes or even considers mitigation techniques. We argue that the future challenge in SDN will be to build active defense mechanisms that are able to take actions in the system to counteract attacks. This will help on bringing new perspectives on how to make secure architectures that are able to detect and automatically counteract threats.

F. COMPREHENSIVE TECHNOLOGICAL REFERENCES

There is not a very large number of adopted technologies to build SDN architectures: these technologies need to be properly documented and referenced to avoid the most common threats. Moreover, we argue that having more variety of available technologies could help to design more secure solutions. Studying new SDN technologies is the starting point to enforce security by design since some of them could be designed to counteract the most known vulnerabilities of the SDN architectures.

G. MACHINE LEARNING

Machine Learning (ML) in its various flavors is strongly considered to develop prevention and detection mechanisms in support of SDN. Recently, some promising ML trends are becoming increasingly popular. Reinforcement Learning (RL) exploits reward functions to train the Machine Learning model to solve vertical problems. RL is not the first choice in SDN right now but we argue that it could be used to train models that are able to reconfigure the network in real-time in order to mitigate the detected attacks.

Adversarial Behaviour is another ML technique that is spreading fast in SDN since it allows to use of this paradigm to simulate attacks that can stress the IDS. We argue that ML will provide even better results if applied to mitigation scenarios since are now only limited to detection and prevention.

H. DENIAL-OF-SERVICE-CENTRIC

Denial of service is the most considered attack in literature. In fact, it is the most dangerous scenario for both the data and control plane, since it is able to fully shut down network devices and compromise connectivity. Other than that, almost every attack considered in the literature that is not necessarily DoS attacks usually follows the behavior of making resources unavailable rather than stealing data or compromising it. Moreover, the works usually do not consider the industrial scenario, which demonstrates how SDN is usually not the first choice for security industrial solutions. We argue that SDN's native features could be exploited to find and track the source of these attacks. This could be done both in data centers and industrial networks, for example with the help of data plane telemetry frameworks that offer standard methodologies to collect data plane statistics in real time. The most famous P4-related telemetry framework is In-band Network Telemetry (INT) [22], which is a valuable starting point.

Also, new flavors of Denial of Service are gaining diffusion recently. Among them, as already mentioned, we can distinguish Low-rate denial of service (LDoS) attacks, which send attacking bursts of packets to degrade the network connectivity, and Economic denial of service (EDoS) attacks, which target cloud environments to inflate the billing of the end user by injecting malicious code into vulnerable machines. This new kind of attack poses various challenges: detecting and mitigating LDoS is not trivial since they follow very unpredictable patterns. New studies should be performed to identify these patterns, perhaps using ML mechanisms. On the other hand, EDoS attacks are difficult to detect since they gain complete access to the resources. For this reason, more effort should be put into designing and analyzing policies to monitor and allow access to cloud resources, exploiting the flexibility and feature of SDN.

I. DISTRIBUTED LEDGERS

The adoption of distributed ledgers and Blockchains can undoubtedly help the security of SDN and Programmable data plane ecosystem in various fields. Certified models and monitoring are performed using a so-called Blockchain layer. Where most publications are focused on Security, there are works on performances

VIII. CONCLUSION

In this article, we presented a systematic review of the literature on SDN security, i.e. work about the security of SDN networks, not about the use of SDN for network security n general.

To conduct our research, we followed a structured approach that allowed us to gather 466 peer-reviewed publications, which, to the best of our knowledge, constitutes the largest curated dataset on the topic.

To study our dataset, we conducted first an investigation on the metadata of the publications, which gave us some insight to map what are the publication outlets, the communities, and the key research concepts that characterize the field. Then, we performed an analysis, associating each element in our dataset to a vector of 14 different markers—presented in the form of 14 research questions. Since our markers belong to four micro-groups (threat model, offensive/defensive goal, infrastructure, and technology), we used that partition to provide an overview of the literature through the lenses of each cluster. As a byproduct of our analysis of the content of each publication, we found concepts and topics that we did not include in our questions but that recur in multiple publications, e.g., the usage of blockchain or Machine Learning technologies. To provide a more comprehensive picture of the field, we described and contextualized also these additional elements. Since our dataset forms a statistically relevant vector field, we also performed a correlation study over the components of the vectors and reported the strongest correlations (e.g., between intrusion detection (IDS) and intrusion-prevention (IPS) systems usage) along with possible explanations of the identified phenomena.

In summary, the analysis of this large amount of papers showed an evident trend in focusing on anti-DoS techniques for Software Defined Networking. Secondly, it showed the absence of an exhaustive threat model, which can effectively respond to the security need of a complex architecture such as SDN. Finally, we noticed a scarce diversity of the technologies adopted in the works present in the dataset, as well as a broad correlation of these studies with Machine Learning solutions and technologies (considering the number of implementations of IDS, IPS, or simple detection/mitigation methodologies).

APPENDIX A ACRONYMS

A. TECHNICAL ACRONYM/GLossario

The following legend is for the acronyms of the journals considered:

SDN Software Defined Networks
NFV Network Function Virtualization
ML Machine Learning
RL Reinforcement Learning
DL Deep Learning
PASTA Process for Attack Simulation and Threat Analysis
STRIDE Spoofing Tampering Repudiation Information disclosure Denial of service Elevation of privilege
DoS Denial of Service
DDoS Distributed Denial of Service
LDoS Low-latency Denial of Service
EDoS Economic Denial of Service
IDS Intrusion Detection System
IPS Intrusion Prevention System

P4 Portal Programmable Pipeline
INT Internet Network Telemetry

B. JOURNALS

The following legend is for the acronyms of the journals considered:

IEEE-Access
CN Computer Networks
NCA Journal of Network and Computer Applications
IJCS International Journal of Communication Systems
TN IEEE/ACM Transactions on Networking
CC Concurrency and Computation: Practice and Experience
IJNM International Journal of Network Management
FGCS Future Generation Computer Systems
ACM/CC Computer Communications
IEEE-IoTJ IEEE Internet of Things Journal
SCN Security and Communication Networks
IEEE-TNSM IEEE Transactions on Network and Service Management
IEEE-JSAC IEEE Journal on Selected Areas in Communications
TETT Transactions on Emerging Telecommunications Technologies
CS Procedia Computer Science
ESA Expert Systems with Applications
C-and-S Computers & Security
IEEE-TIFS IEEE Transactions on Information Forensics and Security
WPC Wireless Personal Communications
FIT Future Internet

C. CONFERENCES

The following legend is for the acronyms of the conferences considered:

Netsoft IEEE International Conference on Network Softwarization
IMCOM International Conference on Ubiquitous Information Management and Communication
SIGSAC ACM SIGSAC Conference on Computer and Communications Security
SysCon IEEE International Systems Conference
FCST International Conference on Frontier of Computer Science and Technology
NFV-SDN IEEE Conference on Network Function Virtualization and Software Defined Networks
ICC IEEE International Conference on Communications
SDN-NFV ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization
SACMAT ACM on Symposium on Access Control Models and Technologies
SOSR Symposium on SDN Research
ICCSP International Conference on Cryptography, Security and Privacy
ICFNDS International Conference on Future Networks and Distributed Systems
CSR International Conference on Cyber Security and Resilience
CCWC IEEE Annual Computing and Communication Workshop and Conference
DISCOVER IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics
SPAC International Conference on Security, Pattern Analysis, and Cybernetics
APNOMS Asia-Pacific Network Operations and Management Symposium
ICCCI International Conference on Computer Communication and Informatics
RIVF RIVF International Conference on Computing and Communication Technologies
CNSM International Conference on Network and Service Management
CONIT International Conference on Intelligent Technologies
ACMI International Conference on Automation, Control, and Mechatronics for Industry 4.0
I2CT International Conference for Convergence in Technology

REFERENCES

[1] S. Ahmad and A. H. Mir, "Scalability, consistency, reliability and security in SDN controllers: A survey of diverse SDN controllers," *J. Netw. Syst. Manage.*, vol. 29, no. 1, pp. 1–59, Jan. 2021.

[2] B. Alhijawi, S. Almajali, H. Elgala, H. B. Salameh, and M. Ayyash, "A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107706.

[3] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, and W. Snow, "ONOS: Towards an open, distributed SDN OS," in *Proc. 3rd Workshop Hot Topics Softw. Defined Netw.*, 2014, pp. 1–6.

[4] A. Clauset, M. E. J. Newman, and C. Moore, "Finding community structure in very large networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 70, no. 6, Dec. 2004, Art. no. 066111.

[5] J. Cohen, "A coefficient of agreement for nominal scales," *Educ. Psychol. Meas.*, vol. 20, no. 1, pp. 37–46, Apr. 1960.

[6] D. Death, *Information Security Handbook: Develop a Threat Model and Incident Response strategy to Build a Strong Information Security Framework*. Birmingham, U.K.: Packt Publishing Ltd, 2017.

[7] R. Deb and S. Roy, "A comprehensive survey of vulnerability and information security in SDN," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108802.

[8] M. Di Pierro, "What is the blockchain?" *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 92–95, 2017.

[9] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments," *IEEE Access*, vol. 7, pp. 80813–80828, 2019.

[10] N. E. Ioini and C. Pahl, "A review of distributed ledger technologies," in *Proc. OTM Confederated Int. Conf. Move Meaningful Internet Syst.* Cham, Switzerland: Springer, 2018, pp. 277–288.

[11] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.

[12] S. Kaur, K. Kumar, N. Aggarwal, and G. Singh, "A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102423.

[13] L. Kohnfelder and P. Garg, *The Threats to Our Products. Microsoft Interface*. Redmond, WA, USA: Microsoft Corporation, 1999.
[14] S. Kyung, W. Han, N. Tiwari, V. H. Dixit, L. Srinivas, Z. Zhao, A. Doupé, and G.-J. Ahn, "HoneyProxy: Design and implementation of next-generation honeynet via SDN," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 1–9.
[15] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.
[16] OWASP Foundation. (Nov. 2020). *Open Web Application Security Project (OWASP) Application Threat Modeling*. [Online]. Available: https://owasp.org/www-community/Application_Threat_Modeling
[17] P. Runeson, M. Höst, A. Rainer, and B. Regnell, *Case Study Research in Software Engineering—Guidelines and Examples*. Hoboken, NJ, USA: Wiley, 2012.
[18] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Comput. Sci. Rev.*, vol. 37, Aug. 2020, Art. no. 100279.
[19] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, Nov. 2019.
[20] J. Soldani, "Grey literature: A safe bridge between academy and industry?" *ACM SIGSOFT Softw. Eng. Notes*, vol. 44, no. 3, pp. 11–12, Nov. 2019.
[21] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-Peer Netw. Appl.*, vol. 12, no. 2, pp. 493–501, Mar. 2019.
[22] L. Tan, W. Su, W. Zhang, J. Lv, Z. Zhang, J. Miao, X. Liu, and N. Li, "In-band network telemetry: A survey," *Comput. Netw.*, vol. 186, Feb. 2021, Art. no. 107763.
[23] O. Tr, "Principles and practices for securing software-defined networks," Open Netw. Found., Palo Alto, CA, USA, Tech. Rep., 2015.
[24] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling*. Hoboken, NJ, USA: Wiley, 2015.
[25] C. Urrea and D. Benítez, "Software-defined networking solutions, architecture and controllers for the industrial Internet of Things: A review," *Sensors*, vol. 21, no. 19, p. 6585, Oct. 2021.
[26] N. J. van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," *Scientometrics*, vol. 84, no. 2, pp. 523–538, Aug. 2010.
[27] O. Yurekten and M. Demirci, "SDN-based cyber defense: A survey," *Future Gener. Comput. Syst.*, vol. 115, pp. 126–149, Feb. 2021.

DATA SET PAPERS

[ds1] Nadine Abbas, Youssef Nasser, Maryam Shehab, and Sanaa Sharafeddine. Attack-specific feature selection for anomaly detection in software-defined networks. In *2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pages 142–146. IEEE, 2021.
[ds2] Nada Mostafa Abd Elazim, Mohamed A Sobh, and Ayman M Bahaa-Eldin. Software defined networking: Attacks and countermeasures. In *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, pages 555–567. IEEE, 2018.
[ds3] AbdelRahman Abdou, Paul C Van Oorschot, and Tao Wan. Comparative analysis of control plane security of sdn and conventional networks. *IEEE Communications Surveys and Tutorials*, 20(4):3542–3559, 2018.
[ds4] Osamah Ibrahiem Abdullaziz and Li-Chun Wang. Mitigating dos attacks against sdn controller using information hiding. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2019.
[ds5] Ihsan H Abdulqadder, Shijie Zhou, Israa T Aziz, Deqing Zou, Xianjun Deng, and Syed Muhammad Abrar Akber. An effective lightweight intrusion detection system with blockchain to mitigate attacks in sdn/nfv enabled cloud. In *2021 6th International Conference for Convergence in Technology (I2CT)*, pages 1–8. IEEE, 2021.
[ds6] Ihsan H Abdulqadder, Shijie Zhou, Deqing Zou, Israa T Aziz, and Syed Muhammad Abrar Akber. Multi-layered intrusion detection and prevention in the sdn/nfv enabled cloud of 5g networks using ai-based defense mechanisms. *Computer Networks*, page 107364, 2020.
[ds7] Ahmed Abusnaina, Aminollah Khormali, DaeHun Nyang, Murat Yuksel, and Aziz Mohaisen. Examining the robustness of learning-based ddos detection in software defined networks. In *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. IEEE, 2019.
[ds8] Stefan Achleitner, Thomas La Porta, Trent Jaeger, and Patrick McDaniel. Adversarial network forensics in software defined networking. In *Proceedings of the Symposium on SDN Research*, pages 8–20. ACM, 2017.
[ds9] Abdulhamid Adebayo and Danda B Rawat. Scalable service-driven database-enabled wireless network virtualization for robust rf sharing. *IEEE Transactions on Services Computing*, pages 1–1, 2021.
[ds10] Yehuda Afek, Anat Bremler-Barr, Shir Landau Feibish, and Liron Schiff. Detecting heavy flows in the sdn match and action model. *Computer Networks*, 136:1–12, 2018.
[ds11] Fatemeh Afghah, Bertrand Cambou, Masih Abedini, and Sherali Zeadally. A reram physically unclonable function (reram puf)-based approach to enhance authentication security in software defined wireless networks. *International Journal of Wireless Information Networks*, 25:117–129, 2018.
[ds12] Neha Agrawal and Shashikala Tapaswi. An sdn-assisted defense mechanism for the shrew ddos attack in a cloud computing environment. *Journal of Network and Systems Management*, 29(2):12, 2021.
[ds13] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, and Andrei Gurtov. Security in software defined networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(4):2317–2346, 2015.
[ds14] Muhammad Ejaz Ahmed, Hyoungshick Kim, and Moosung Park. Mitigating dns query-based ddos attacks with machine learning on software-defined networking. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pages 11–16. IEEE, 2017.
[ds15] Usama Ahmed, Imran Raza, Syed Asad Hussain, Amjad Ali, Muddesar Iqbal, and Xinheng Wang. Modelling cyber security for software-defined networks those grow strong when exposed to threats: Analysis and propositions. *Journal of reliable intelligent environments*, 1:123–146, 2015.
[ds16] Nisha Ahuja, Gaurav Singal, and Debajyoti Mukhopadhyay. Dlsdn: Deep learning for ddos attack detection in software defined networking. In *2021 11th International Conference on Cloud Computing, Data Science and Engineering (Confluence)*, pages 683–688. IEEE, 2021.
[ds17] James Aiken and Sandra Scott-Hayward. Investigating adversarial attacks against network intrusion detection systems in sdns. In *2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–7. IEEE, 2019.
[ds18] Ahmad Ariff Aizuddin, Mohd Atan, Megat Norulazmi, Megat Mohamed Noor, Shadil Akimi, and Zainal Abidin. Dns amplification attack detection and mitigation via sflow with security-centric sdn. In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, pages 1–7. ACM, 2017.
[ds19] Adnan Akhunzada, Abdullah Gani, Nor Badrul Anuar, Ahmed Abdelaziz, Muhammad Khurram Khan, Amir Hayat, and Samee U Khan. Secure and dependable software defined networks. *Journal of Network and Computer Applications*, 61:199–221, 2016.
[ds20] Basheer Al-Duwairi, Eslam Al-Quraan, and Yazeed AbdelQader. Isdsdn: mitigating syn flood attacks in software defined networks. *Journal of Network and Systems Management*, 28:1366–1390, 2020.
[ds21] Abdussalam Ahmed Alashhab, Mohd Soperi Mohd Zahid, Ali Ahmed Barka, and Abobaker M Albaboh. Experimenting and evaluating the impact of dos attacks on different sdn controllers. In *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, pages 722–727. IEEE, 2021.
[ds22] Ahmed AlEroud and Izzat Alsmadi. Identifying cyber-attacks on software defined networks: An inference-based intrusion detection approach. *Journal of Network and Computer Applications*, 80:152–164, 2017.
[ds23] Talal Alharbi, Siamak Layeghy, and Marius Portmann. Experimental evaluation of the impact of dos attacks in sdn. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6. IEEE, 2017.
[ds24] Mohammad Alhisnawi and Mahmood Ahmadi. Detecting and mitigating ddos attack in named data networking. *Journal of Network and Systems Management*, 28(4):1343–1365, 2020.
[ds25] Amir Ali and Muhammad Murtaza Yousaf. Novel three-tier intrusion detection and prevention system in software defined network. *IEEE Access*, 8:109662–109676, 2020.
[ds26] Belal Ali, Mark A Gregory, and Shuo Li. Multi-access edge computing architecture, data security and privacy: A review. *IEEE Access*, 9:18706–18721, 2021.

[ds27] Sarwan Ali, Maria Khalid Alvi, Safi Faizullah, Muhammad Asad Khan, Abdullah Alshanqiti, and Imdadullah Khan. Detecting ddos attack on sdn due to vulnerabilities in openflow. In *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*, pages 1–6. IEEE, 2020.

[ds28] Aliyu Lawal Aliyu, Adel Aneiba, Mohamed Patwary, and Peter Bull. A trust management framework for software defined network (sdn) controller and network applications. *Computer Networks*, page 107421, 2020.

[ds29] Ibrahim Aliyu, Marco Carlo Feliciano, Sélinde Van Engelenburg, Dong Ok Kim, and Chang Gyoon Lim. A blockchain-based federated forest for sdn-enabled in-vehicle network intrusion detection system. *IEEE Access*, 9:102593–102608, 2021.

[ds30] Fahad M. Alotaibi and Vassilios G. Vassilakis. Sdn-based detection of self-propagating ransomware: The case of badrabbit. *IEEE Access*, 9:28039–28058, 2021.

[ds31] Abdulrahman Saad Alqahtani. Security threats and countermeasures in software defined network using efficient and secure trusted routing mechanism. *Computer Communications*, 153:336–341, 2020.

[ds32] Adel Alshamrani, Ankur Chowdhary, Sandeep Pisharody, Duo Lu, and Dijiang Huang. A defense system for defeating ddos attacks in sdn based networks. In *Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access*, pages 83–92, 2017.

[ds33] Abdullah Soliman Alshra'a and Jochen Seitz. External device to protect the software-defined network performance in case of a malicious attack. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pages 1–6. ACM, 2019.

[ds34] Izzat Alsmadi and Dianxiang Xu. Security of software defined networks: A survey. *Computers and security*, 53:79–108, 2015.

[ds35] Moreno Ambrosin, Mauro Conti, Fabio De Gaspari, and Radha Poovendran. Lineswitch: Efficiently managing switch flow in software-defined networking while effectively tackling dos attacks. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pages 639–644, 2015.

[ds36] Moreno Ambrosin, Mauro Conti, Fabio De Gaspari, and Radha Poovendran. Lineswitch: Tackling control plane saturation attacks in software-defined networking. *IEEE/ACM Transactions on Networking*, 25(2):1206–1219, 2016.

[ds37] Ruhul Amin, Isha Pali, and Venkatasamy Sureshkumar. Software-defined network enabled vehicle to vehicle secured data transmission protocol in vanets. *Journal of Information Security and Applications*, 58:102729, 2021.

[ds38] N Anand, Sarath Babu, and BS Manoj. On detecting compromised controller in software defined networks. *Computer Networks*, 137:107–118, 2018.

[ds39] Septha Anggara, Hilal Hudan Nuha, and Muhammad Agus Triawan. Effect of binding attack on software defined network. In *2021 7th International Conference on Education and Technology (ICET)*, pages 152–155. IEEE, 2021.

[ds40] Iffat Anjum, Mu Zhu, Isaac Polinsky, William Enck, Michael K. Reiter, and Munindar Singh. Role-based deception in enterprise networks, 2020.

[ds41] Daniele Antonioli and Nils Ole Tippenhauer. Minicps: A toolkit for security research on cps networks. In *Proceedings of the First ACM workshop on cyber-physical systems-security and/or privacy*, pages 91–100, 2015.

[ds42] D Arivudainambi, Varun Kumar KA, and S Sibi Chakkaravarthy. Lion ids: A meta-heuristics approach to detect ddos attacks against software-defined networks. *Neural Computing and Applications*, 31:1491–1501, 2019.

[ds43] Ahmed Arsalan and Rana Asif Rehman. Prevention of timing attack in software defined named data network with vanets. In *2018 International Conference on Frontiers of Information Technology (FIT)*, pages 247–252. IEEE, 2018.

[ds44] Ahmad Aseeri, Nuttapong Netjinda, and Rattikorn Hewett. Alleviating eavesdropping attacks in software-defined networking data plane. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, pages 1–8. ACM, 2017.

[ds45] Javed Ashraf, N Moustafa, Asim D Bukhshi, and Abdullah Javed. Intrusion detection system for sdn-enabled iot networks using machine learning techniques. In *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)*, pages 46–52. IEEE, 2021.

[ds46] Sumit Badotra and Surya Narayan Panda. Snort based early ddos detection system using opendaylight and open networking operating system in software defined networking. *Cluster Computing*, 24:501–513, 2021.

[ds47] Jan Badshah, Muhammad Kamran, Nadir Shah, and Shahbaz Akhtar Abid. An improved method to deploy cache servers in software defined network-based information centric networking for big data. *Journal of Grid Computing*, 17:255–277, 2019.

[ds48] Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, and Sithamparanathan Kandeepan. Dynamics of botnet propagation in software defined networks using epidemic models. *IEEE Access*, 9:119406–119417, 2021.

[ds49] Shruti Banerjee and Partha Sarathi Chakraborty. To detect the distributed denial-of-service attacks in sdn using machine learning algorithms. In *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 966–971, 2021.

[ds50] Lohit Barki, Amrit Shidling, Nisharani Meti, DG Narayan, and Mohammed Moin Mulla. Detection of distributed denial of service attacks in software defined networks. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 2576–2581. IEEE, 2016.

[ds51] K Bavani, MP Ramkumar, and Emil Selvan GSR. Statistical approach based detection of distributed denial of service attack in a software defined network. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 380–385. IEEE, 2020.

[ds52] Narmeen Zakaria Bawany, Jawwad A Shamsi, and Khaled Salah. Ddos attack detection and mitigation using sdn: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 42:425–441, 2017.

[ds53] Jaouad Benabbou, Khalid Elbaamrani, and Noureddine Idboufker. Security in openflow-based sdn, opportunities and challenges. *Photonic Network Communications*, 37:1–23, 2019.

[ds54] Faycal Bensalah, Najib El Kamoun, and Mohammed-Alamine El Houssaini. Inline detection of denial of service attacks in software defined networking using the hotelling chart. *Procedia Computer Science*, 160:785–790, 2019.

[ds55] Davide Berardi, Franco Callegati, Andrea Melis, and Marco Prandini. Security network policy enforcement through a sdn framework. In *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–4. IEEE, 2018.

[ds56] Vidhi Bhavsar, Chairunnisa Sahrial, and Bhargavi Goswami. Security and performance evaluation of software defined network controllers against distributed denial of service attack. In *2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pages 1–8, 2021.

[ds57] Jalal Bhayo, Riaz Jafaq, Awais Ahmed, Sufian Hameed, and Syed Attique Shah. A time-efficient approach towards ddos attack detection in iot network using sdn. *IEEE Internet of Things Journal*, 2021.

[ds58] Kriti Bhushan and Brij B Gupta. Distributed denial of service (ddos) attack mitigation in software defined network (sdn)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, 10:1985–1997, 2019.

[ds59] Shanshan Bian, Peng Zhang, and Zheng Yan. A survey on software-defined networking security. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, pages 190–198. ACM, 2016.

[ds60] PK Binu, Deepak Mohan, and EM Sreerag Haridas. An sdn-based prototype for dynamic detection and mitigation of dos attacks in iot. In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, pages 5–10. IEEE, 2021.

[ds61] Celyn Birkinshaw, Elpida Rouka, and Vassilios G Vassilakis. Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *Journal of Network and Computer Applications*, 136:71–85, 2019.

[ds62] Conor Black and Sandra Scott-Hayward. A survey on the verification of adversarial data planes in software-defined networks. In *Proceedings of the 2021 ACM International Workshop on Software Defined Networks and Network Function Virtualization Security*, SDN-NFV Sec'21, page 3–10, New York, NY, USA, 2021. Association for Computing Machinery.

[ds63] Alessandro Bocci, Stefano Forti, Gian-Luigi Ferrari, and Antonio Brogi. Secure faas orchestration in the fog: how far are we? *Computing*, 103(5):1025–1056, 2021.

[ds64] Nurefşan Sertbaş Bülbül and Mathias Fischer. Sdn/nfv-based ddos mitigation via pushback. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

[ds65] Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski, and Piotr Żórawski. Sdn-based mitigation of scanning attacks for the 5g internet of radio light system. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–10. ACM, 2018.

[ds66] Gui-lin Cai, Bao-sheng Wang, Wei Hu, and Tian-zuo Wang. Moving target defense: state of the art and characteristics. *Frontiers of Information Technology & Electronic Engineering*, 17(11):1122–1153, 2016.

[ds67] Yun-Zhan Cai, Ting-Yu Lin, Yu-Ting Wang, Ya-Pei Tuan, and Meng-Hsun Tsai. E-replacement: Efficient scanner data collection method in p4-based software-defined networks. *International Journal of Network Management*, 31(6):e2162, 2021.

[ds68] Yongyi Cao, Hao Jiang, Yuchuan Deng, Jing Wu, Pan Zhou, and Wei Luo. Detecting and mitigating ddos attacks in sdn using spatial-temporal graph convolutional network. *IEEE Transactions on Dependable and Secure Computing*, 2021.

[ds69] Luiz Fernando Carvalho, Taufik Abrão, Leonardo de Souza Mendes, and Mario Lemes Proença Jr. An ecosystem for anomaly detection and mitigation in software-defined networking. *Expert Systems with Applications*, 104:121–133, 2018.

[ds70] Ranyelson N Carvalho, Lucas R Costa, Jacir L Bordim, and Eduardo AP Alchieri. Detecting ddos attacks on sdn data plane with machine learning. In *2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW)*, pages 138–144. IEEE, 2021.

[ds71] Ranyelson Neres Carvalho, Jacir Luiz Bordim, and Eduardo Adilio Pelinson Alchieri. Entropy-based dos attack identification in sdn. In *2019 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, pages 627–634. IEEE, 2019.

[ds72] Durbadal Chattaraj, Basudeb Bera, Ashok Kumar Das, Joel JPC Rodrigues, and Youngho Park. Designing fine-grained access control for software-defined networks using private blockchain. *IEEE Internet of Things Journal*, 9(2):1542–1559, 2021.

[ds73] Chih-Chieh Chen, Yi-Ren Chen, Wei-Chih Lu, Shi-Chun Tsai, and Ming-Chuan Yang. Detecting amplification attacks with software defined networking. In *2017 IEEE conference on dependable and secure computing*, pages 195–201. IEEE, 2017.

[ds74] Jing Chen, Xi Cheng, Ruiying Du, Li Hu, and Chiheng Wang. Botguard: Lightweight real-time botnet detection in software defined networks. *Wuhan University Journal of Natural Sciences*, 22(2):103–113, 2017.

[ds75] K. Chen, S. Liu, Y. Xu, I. Siddhrau, S. Zhou, Z. Guo, and H. Chao. Sdnshield: Nfv-based defense framework against ddos attacks on sdn control plane. *IEEE/ACM Transactions on Networking*, (01):1–17, 5555.

[ds76] Min Chen, Yongfeng Qian, Shiwen Mao, Wan Tang, and Ximin Yang. Software-defined mobile networks security. *Mobile Networks and Applications*, 21:729–743, 2016.

[ds77] Ming-Hung Chen, Jyun-Yan Ciou, I-Hsin Chung, and Cheng-Fu Chou. Flexprotect: A sdn-based ddos attack protection architecture for multi-tenant data centers. In *Proceedings of the International Conference on High Performance Computing in Asia-Pacific Region*, pages 202–209. ACM, 2018.

[ds78] Shuhan Chen, Congqi Shen, Danrui Yu, Yuqin Wu, and Chunming Wu. Intelligent ddos detection in botnet combined with packet-level features under sdn. In *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE.

[ds79] Yen-Hung Chen, Pi-Tzong Jan, Ching-Neng Lai, ChunWei Huang, Chih-Han Chang, and Yo-Cih Huang. Detecting linking flooding attacks using deep convolution network. In *Proceedings of the 2020 the 3rd International Conference on Computers in Management and Business*, pages 70–74. ACM, 2020.

[ds80] Shoya Chiba, Luis Guillen, Satoru Izumi, Toru Abe, and Takuo Suganuma. Design of a network scan defense method by combining an sdn-based mtd and ips. In *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 273–278. IEEE, 2021.

[ds81] Juan Camilo Correa Chica, Jenny Cuatindioy Imbachi, and Juan Felipe Botero. Security in sdn: A comprehensive survey. *Journal of Network and Computer Applications*, page 102595, 2020.

[ds82] Ankur Chowdhary, Adel Alshamrani, Dijiang Huang, and Hongbin Liang. Mtd analysis and evaluation framework in software defined network (mason). In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization*, pages 43–48, 2018.

[ds83] Mauro Conti, Fabio De Gaspari, and Luigi Vincenzo Mancini. A novel stealthy attack to gather sdn configuration-information. *IEEE Transactions on Emerging Topics in Computing*, 2018.

[ds84] Mauro Conti, Ankit Gangwal, and Manoj Singh Gaur. A comprehensive and effective mechanism for ddos detection in sdn. In *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–8. IEEE, 2017.

[ds85] Mauro Conti, Chhagan Lal, Reza Mohammadi, and Umashankar Rawat. Lightweight solutions to counter ddos attacks in software defined networking. *Wireless Networks*, 25:2751–2768, 2019.

[ds86] Jie Cui, Mingjun Wang, Yonglong Luo, and Hong Zhong. Ddos detection and defense mechanism based on cognitive-inspired computing in sdn. *Future Generation Computer Systems*, 97:275–283, 2019.

[ds87] Yunhe Cui, Lianshan Yan, Saifei Li, Huanlai Xing, Wei Pan, Jian Zhu, and Xiaoyang Zheng. Sd-anti-ddos: Fast and efficient ddos defense in software-defined networks. *Journal of Network and Computer Applications*, 68:65–79, 2016.

[ds88] Weverton Luis da Costa Cordeiro, Jonatas Adilson Marques, and Luciano Paschoal Gaspary. Data plane programmability beyond openflow: Opportunities and challenges for network and service operations and management. *Journal of Network and Systems Management*, 25:784–818, 2017.

[ds89] Anderson Santos da Silva, Paul Smith, Andreas Mauthe, and Alberto Schaeffer-Filho. Resilience support in software-defined networking: A survey. *Computer Networks*, 92:189–207, 2015.

[ds90] Delali Kwasi Dake, James Dzisi Gadze, and Griffith Selorm Klogo. Ddos and flash event detection in higher bandwidth sdn-iot using multiagent reinforcement learning. In *2021 International Conference on Computing, Computational Modelling and Applications (ICCMA)*, pages 16–20. IEEE, 2021.

[ds91] Bruno L Dalmazo, Jonatas A Marques, Lucas R Costa, Michel S Bonfim, Ranyelson N Carvalho, Anderson S da Silva, Stenio Fernandes, Jacir L Bordim, Eduardo Alchieri, Alberto Schaeffer-Filho, et al. A systematic review on distributed denial of service attack defense mechanisms in programmable networks. *International Journal of Network Management*, 31(6):e2163, 2021.

[ds92] Pascal Dauer, Rahamatullah Khondoker, Ronald Marx, and Kpatcha Bayarou. Security analysis of software defined networking applications for monitoring and measurement: Sflow and bigtap. In *The 10th international conference on future internet*, pages 51–56. ACM, 2015.

[ds93] Neelam Dayal, Prasenjit Maity, Shashank Srivastava, and Rahamatullah Khondoker. Research trends in security and ddos in sdn. *Security and Communication Networks*, 9(18):6386–6411, 2016.

[ds94] Neelam Dayal and Shashank Srivastava. Analyzing behavior of ddos attacks to identify ddos detection features in sdn. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*, pages 274–281. IEEE, 2017.

[ds95] Neelam Dayal and Shashank Srivastava. An rbf-pso based approach for early detection of ddos attacks in sdn. In *2018 10th International Conference on Communication Systems and Networks (COMSNETS)*, pages 17–24. IEEE, 2018.

[ds96] Marcos VO De Assis, Matheus P Novaes, Cinara B Zerbini, Luiz F Carvalho, Taufik Abrãao, and Mario L Proença. Fast defense system against attacks in software defined networks. *IEEE Access*, 6:69620–69639, 2018.

[ds97] Raktim Deb and Sudipta Roy. A software defined network information security risk assessment based on pythagorean fuzzy sets. *Expert Systems with Applications*, 183:115383, 2021.

[ds98] Shuhua Deng, Xing Gao, Zebin Lu, Zhengfa Li, and Xieping Gao. Dos vulnerabilities and mitigation strategies in software-defined networks. *Journal of Network and Computer Applications*, 125:209–219, 2019.

[ds99] Phuc Trinh Dinh and Minho Park. Bdf-sdn: A big data framework for ddos attack detection in large-scale sdn-based cloud. In *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. IEEE, 2021.

[ds100] Phuc Trinh Dinh and Minho Park. Economic denial of sustainability (edos) detection using gans in sdn-based cloud. In *2020 IEEE Eighth International Conference on Communications and Electronics (ICCE)*, pages 135–140. IEEE, 2021.

[ds101] Vaibhav Hemant Dixit, Adam Doupé, Yan Shoshitaishvili, Ziming Zhao, and Gail-Joon Ahn. Aim-sdn: attacking information mismanagement in sdn-datastores. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 664–676, 2018.

[ds102] Hien Do Hoang, Van-Hau Pham, et al. Empirical study on reconnaissance attacks in sdn-aware network for evaluating cyber deception. In *2021 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pages 1–6. IEEE, 2021.

[ds103] Lobna Dridi and Mohamed Faten Zhani. A holistic approach to mitigating dos attacks in sdn networks. *International Journal of Network Management*, 28(1):e1996, 2018.

[ds104] Phan The Duy, Le Duy An, and Van-Hau Pham. Mitigating flow table overloading attack with controller-based flow filtering strategy in sdn. In *Proceedings of the 2019 the 9th International Conference on Communication and Network Security*, pages 154–158. ACM, 2019.

[ds105] Ali El Kamel, Hamdi Eltaief, and Habib Youssef. On-the-fly (d)dos attack mitigation in sdn using deep neural network-based rate limiting. *Computer Communications*, 182:153–169, 2022.

[ds106] Mahmoud Elhejazi and Mohamed Musbah. Dynamic defense in-depth model for sdn control layer to enhance openflow protocol security. In *The 7th International Conference on Engineering and MIS 2021*, ICEMIS'21, New York, NY, USA, 2021. Association for Computing Machinery.

[ds107] Mahmoud Said ElSayed, Nhien-An Le-Khac, Marwan Ali Albahar, and Anca Jurcut. A novel hybrid model for intrusion detection systems in sdns based on cnn and a new regularization technique. *Journal of Network and Computer Applications*, 191:103160, 2021.

[ds108] Zhijie Fan, Ya Xiao, Amiya Nayak, and Chengxiang Tan. An improved network security situation assessment approach in software defined networks. *Peer-to-Peer Networking and Applications*, 12:295–309, 2019.

[ds109] Awatef Ali Yousef R Fares, Francisco L de Caldas Filho, William F Giozza, Edna Dias Canedo, Fábio Lúcio Lopes de Mendonça, and Georges Daniel Amvame Nze. Dos attack prevention on ips sdn networks. In *2019 Workshop on Communication Networks and Power Systems (WCNPS)*, pages 1–7. IEEE, 2019.

[ds110] Muhammad Usman Farooq, Muhammad Rashid, Farooque Azam, Yawar Rasheed, Muhammad Waseem Anwar, and Zohaib Shahid. A model-driven framework for the prevention of dos attacks in software defined networking (sdn). In *2021 IEEE International Systems Conference (SysCon)*, pages 1–7. IEEE, 2021.

[ds111] Kiran Fatima, Kanwal Zahoor, and Narmeen Zakaria Bawany. Sdn control plane security: Attacks and mitigation techniques. In *Proceedings of the 4th International Conference on Networking, Information Systems and Security*, NISS2021, New York, NY, USA, 2021. Association for Computing Machinery.

[ds112] Huifen Feng, Xincheng Yan, Na Zhou, Zhihong Jiang, and Ying Liu. A cross-domain collaborative ddos defense scheme based on blockchain-sdn in the iot. In *Proceedings of the 2021 ACM International Conference on Intelligent Computing and Its Emerging Applications*, ACM ICEA '21, page 77–82, New York, NY, USA, 2022. Association for Computing Machinery.

[ds113] Jon Gabirondo-López, Jon Ega±a, Jose Miguel-Alonso, and Raul Orduna Urrutia. Towards autonomous defense of sdn networks using muzero based intelligent agents. *IEEE Access*, 9:107184–107199, 2021.

[ds114] Jesús Galeano-Brajones, David Cortés-Polo, Juan F Valenzuela-Valdés, Antonio M Mora, and Javier Carmona-Murillo. Detection and mitigation of dos attacks in sdn. an experimental approach. In *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pages 575–580. IEEE, 2019.

[ds115] Aparna Ganesan and Kamil Sarac. Mitigating evasion attacks on machine learning based nids systems in sdn. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, pages 268–272. IEEE, 2021.

[ds116] Shang Gao, Zhe Peng, Bin Xiao, Aiqun Hu, Yubo Song, Kui Ren, et al. Detection and mitigation of dos attacks in software defined networks. *IEEE/ACM Transactions on Networking*, 2020.

[ds117] Norberto Garcia, Tomas Alcaniz, Aurora González-Vidal, Jorge Bernal Bernabe, Diego Rivera, and Antonio Skarmeta. Distributed real-time slowdos attacks detection over encrypted traffic using artificial intelligence. *Journal of Network and Computer Applications*, 173:102871, 2021.

[ds118] Joe Gardiner, Awais Rashid, Shishir Nagaraja, Peter Garraghan, Nicholas Race, and Adam Eiffert. Controller-in-the-middle: Attacks on software defined networks in industrial control systems. In *The 2nd Joint Workshop on CPS and IoT Security and Privacy (CPSIoTSec 21)*. ACM Press / Sheridan, 2021.

[ds119] Yubaraj Gautam, Kazuhiko Sato, Bishnu Prasad Gautam, and Norio Shiratori. Novel firewall application for mitigating flooding attacks on an sdn network. In *2021 International Conference on Networking and Network Applications (NaNA)*, pages 449–455. IEEE, 2021.

[ds120] R Geetha, AK Suntheya, and G Umarani Srikanth. Cloud integrated iot enabled sensor network security: research issues and solutions. *Wireless Personal Communications*, 113:747–771, 2020.

[ds121] Manuel Gil Pérez, Alberto Huertas Celdrán, Pietro G Giardina, Giacomo Bernini, Simone Pizzimenti, Félix J García Clemente, Gregorio Martínez Perez, Giovanni Festa, and Fabio Paglianti. Mitigation of cyber threats: Protection mechanisms in federated sdn/nfv infrastructures for 5g within fire+. *Concurrency and Computation: Practice and Experience*, page e5132, 2019.

[ds122] Fida Gillani, Ehab Al-Shaer, and Qi Duan. In-design resilient sdn control plane and elastic forwarding against aggressive ddos attacks. In *Proceedings of the 5th ACM Workshop on Moving Target Defense*, pages 80–89, 2018.

[ds123] Kostas Giotis, George Androulidakis, and Vasilis Maglaris. A scalable anomaly detection and mitigation architecture for legacy networks via an openflow middlebox. *Security and Communication Networks*, 9(13):1958–1970, 2016.

[ds124] Kostas Giotis, Maria Apostolaki, and Vasilis Maglaris. A reputation-based collaborative schema for the mitigation of distributed attacks in sdn domains. In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, pages 495–501. IEEE, 2016.

[ds125] Thomas Girdler and Vassilios G Vassilakis. Implementing an intrusion detection and prevention system using software-defined networking: defending against arp spoofing attacks and blacklisted mac addresses. *Computers and Electrical Engineering*, 90:106990, 2021.

[ds126] Christos Gkountis, Miran Taha, Jaime Lloret, and Georgios Kambourakis. Lightweight algorithm for protecting sdn controller against ddos attacks. In *2017 10th IFIP Wireless and Mobile Networking Conference (WMNC)*, pages 1–6. IEEE, 2017.

[ds127] Nail Goksel and Mehmet Demirci. Dos attack detection using packet statistics in sdn. In *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE, 2019.

[ds128] Changqing Gong, Delong Yu, Liang Zhao, Xiguang Li, and Xianwei Li. An intelligent trust model for hybrid ddos detection in software defined networks. *Concurrency and Computation: Practice and Experience*, 32(16):e5264, 2020.

[ds129] Yili Gong, Wei Huang, Wenjie Wang, and Yingchun Lei. A survey on software defined networking and its applications. *Frontiers of Computer Science*, 9:827–845, 2015.

[ds130] Holden Gordon, Christopher Batula, Bhagyashri Tushir, Behnam Dezfouli, and Yuhong Liu. Securing smart homes via software-defined networking and low-cost traffic classification. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1049–1057, 2021.

[ds131] Yi Guo, Fu Miao, Liancheng Zhang, and Yu Wang. Cath: An effective method for detecting denial-of-service attacks in software defined networks. *Science China Information Sciences*, 62(3):32106, 2019.

[ds132] SUN Guozi, Wenti Jiang, GU Yu, REN Danni, and LI Huakang. Ddos attacks and flash event detection based on flow characteristics in sdn. In *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 1–6. IEEE, 2018.

[ds133] Shaveta Gupta and Dinesh Grover. A comprehensive review on detection of ddos attacks using ml in sdn environment. In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pages 1158–1163, 2021.

[ds134] Vishal Gupta, Amrit Kochar, Shail Saharan, and Rakhee Kulshrestha. Dns amplification based ddos attacks in sdn environment: Detection and mitigation. In *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, pages 473–478. IEEE, 2019.

[ds135] UmaMaheswari Gurusamy and Manikandan MSK. Detection and mitigation of udp flooding attack in a multicontroller software defined network using secure flow management model. *Concurrency and Computation: Practice and Experience*, 31(20):e5326, 2019.

[ds136] Taejin Ha, Sunghwan Kim, Namwon An, Jargalsaikhan Narantuya, Chiwook Jeong, JongWon Kim, and Hyuk Lim. Suspicious traffic sampling for intrusion detection in software-defined networks. *Computer Networks*, 109:172–182, 2016.

[ds137] Sufian Hameed and Hassan Ahmed Khan. Leveraging sdn for collaborative ddos mitigation. In *2017 International Conference on Networked Systems (NetSys)*, pages 1–6. IEEE, 2017.

[ds138] Tao Han, Syed Rooh Ullah Jan, Zhiyuan Tan, Muhammad Usman, Mian Ahmad Jan, Rahim Khan, and Yongzhao Xu. A comprehensive survey of security threats and their mitigation techniques for next-generation sdn controllers. *Concurrency and Computation: Practice and Experience*, 32(16):e5300, 2020.

[ds139] Wonkyu Han, Hongxin Hu, Ziming Zhao, Adam Doupé, Gail-Joon Ahn, Kuang-Ching Wang, and Juan Deng. State-aware network access management for software-defined networks. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*, pages 1–11, 2016.

[ds140] Vikas Hassija, Vinay Chamola, Adhar Agrawal, Adit Goyal, Nguyen Cong Luong, Dusit Niyato, F Richard Yu, and Mohsen Guizani. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 2021.

[ds141] Hien Do Hoang, Phan The Duy, and Van-Hau Pham. A security-enhanced monitoring system for northbound interface in sdn using blockchain. In *Proceedings of the Tenth International Symposium on Information and Communication Technology*, pages 197–204. ACM, 2019.

[ds142] Hanshu Hong and Zhixin Sun. Applying sdn for data extraction and mining: an enhanced architecture. *National Academy Science Letters*, 40:167–169, 2017.

[ds143] Jianwei Hou, Minjian Zhang, Ziqi Zhang, Wenchang Shi, Bo Qin, and Bin Liang. On the fine-grained fingerprinting threat to software-defined networks. *Future Generation Computer Systems*, 107:485–497, 2020.

[ds144] Bing Hu, Yuanguo Bi, Mingjian Zhi, Kuan Zhang, Feihong Yan, Qian Zhang, and Zheng Liu. A deep one-class intrusion detection scheme in software-defined industrial networks. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, 18(6), 2022.

[ds145] Dingwen Hu, Peilin Hong, and Yixin Chen. Fadm: Ddos flooding attack detection and mitigation system in software-defined networking. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–7. IEEE, 2017.

[ds146] Hongxin Hu, Wonkyu Han, Sukwha Kyung, Juan Wang, Gail-Joon Ahn, Ziming Zhao, and Hongda Li. Towards a reliable firewall for software-defined networks. *Computers and Security*, 87:101597, 2019.

[ds147] Tao Hu, Peng Yi, Julong Lan, Yuxiang Hu, and Penghao Sun. Acst: Audit-based compromised switch tolerance for enhancing data plane robustness in software-defined networking. *Computer Networks*, 161:264–280, 2019.

[ds148] Jingyu Hua, Zidong Zhou, and Sheng Zhong. Flow misleading: Wormhole attack in software-defined networking via building in-band covert channel. *IEEE Transactions on Information Forensics and Security*, 16:1029–1043, 2020.

[ds149] Haiou Huang, Jianfeng Chu, and Xiaochun Cheng. Trend analysis and countermeasure research of ddos attack under 5g network. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pages 153–160, 2021.

[ds150] Weigui Huang, Yifeng Sun, Wang Ou, and Yubin Wang. A flow scheduling model for sdn honeypot using multi-layer attack graphs and signaling game. In *2021 7th International Conference on Computer and Communications (ICCC)*, pages 2012–2020. IEEE, 2021.

[ds151] Xinli Huang, Peng Shi, Yufei Liu, and Fei Xu. Towards trusted and efficient sdn topology discovery: A lightweight topology verification scheme. *Computer Networks*, 170:107119, 2020.

[ds152] Xueli Huang, Xiaojiang Du, and Bin Song. An effective ddos defense scheme for sdn. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2017.

[ds153] Truong Thu Huong and Nguyen Huu Thanh. Software defined networking-based one-packet ddos mitigation architecture. In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, pages 1–7. ACM, 2017.

[ds154] Ali Hussein, Imad H Elhajj, Ali Chehab, and Ayman Kayssi. Sdn security plane: An architecture for resilient security services. In *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, pages 54–59. IEEE, 2016.

[ds155] Henan Kottayil Hyder and Chung-Horng Lung. Closed-loop ddos mitigation system in software defined networks. In *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–6. IEEE, 2018.

[ds156] Muhammad Faraz Hyder and Tasbiha Fatima. Towards crossfire distributed denial of service attack protection using intent-based moving target defense over software-defined networking. *IEEE Access*, 9:112792–112804, 2021.

[ds157] Muhammad Faraz Hyder and Muhammad Ali Ismail. Securing control and data planes from reconnaissance attacks using distributed shadow controllers, reactive and proactive approaches. *IEEE Access*, 9:21881–21894, 2021.

[ds158] Muhammad Faraz Hyder and Muhammad Ali Ismail. Toward domain name system privacy enhancement using intent-based moving target defense framework over software defined networks. *Transactions on Emerging Telecommunications Technologies*, 32(10):e4318, 2021.

[ds159] Poulmanogo Illy, Georges Kaddoum, Kuljeet Kaur, and Sahil Garg. Ml-based idps enhancement with complementary features for home iot networks. *IEEE Transactions on Network and Service Management*, 2022.

[ds160] Muhammad Imran, Muhammad Hanif Durad, Farrukh Aslam Khan, and Haider Abbas. Daisy: A detection and mitigation system against denial-of-service attacks in software-defined networks. *IEEE Systems Journal*, 2019.

[ds161] Muhammad Imran, Muhammad Hanif Durad, Farrukh Aslam Khan, and Abdelouahid Derhab. Toward an optimal solution against denial of service attacks in software defined networks. *Future Generation Computer Systems*, 92:444–453, 2019.

[ds162] Waseem Iqbal, Haider Abbas, Bilal Rauf, Yawar Abbas, Faisal Amjad, and Ahmed Hemani. Pcss: Privacy preserving communication scheme for sdn enabled smart homes. *IEEE Sensors Journal*, pages 1–1, 2021.

[ds163] Vinay Itagi, Mayur Javali, H Madhukeshwar, Pooja Shettar, P Somashekar, and DG Narayan. Ddos attack detection in sdn environment using bi-directional recurrent neural network. In *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, pages 123–128. IEEE, 2021.

[ds164] Tohid Jafarian, Mohammad Masdari, Ali Ghaffari, and Kambiz Majidzadeh. Security anomaly detection in software-defined networking based on a prediction technique. *International Journal of Communication Systems*, 33(14):e4524, 2020.

[ds165] Tohid Jafarian, Mohammad Masdari, Ali Ghaffari, and Kambiz Majidzadeh. A survey and classification of the security anomaly detection mechanisms in software defined networks. *Cluster Computing*, 24:1235–1253, 2021.

[ds166] Saksit Jantila and Kornchawal Chaipah. A security analysis of a hybrid mechanism to defend ddos attacks in sdn. *Procedia Computer Science*, 86:437–440, 2016.

[ds167] Forough Ja'fari, Seyedakbar Mostafavi, Kiarash Mizanian, and Emad Jafari. An intelligent botnet blocking approach in software defined networks using honeypots. *Journal of Ambient Intelligence and Humanized Computing*, 12:2993–3016, 2021.

[ds168] Stefan Jevtic, Hamidreza Lotfalizadeh, and Dongsoo S Kim. Toward network-based ddos detection in software-defined networks. In *Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication*, pages 1–8. ACM, 2018.

[ds169] Maria B Jimenez, David Fernandez, Jorge Eduardo Rivadeneira, Luis Bellido, and Andres Cardenas. A survey of the main security issues and solutions for the sdn architecture. *IEEE Access*, 9:122016–122038, 2021.

[ds170] Yong Jin, Masahiko Tomoishi, and Nariyoshi Yamai. Anomaly detection on user terminals based on outbound traffic filtering by dns query monitoring and application program identification. In *2021 International Conference on Human-Machine Interaction*, ICHMI 2021, page 47–56, New York, NY, USA, 2021. Association for Computing Machinery.

[ds171] Abdellah Kaci and Abderrezak Rachedi. Toward a machine learning and software defined network approaches to manage miners' reputation in blockchain. *Journal of Network and Systems Management*, 28:478–501, 2020.

[ds172] Kübra Kalkan, Levent Altay, Gürkan Gür, and Fatih Alagöz. Jess: Joint entropy-based ddos defense scheme in sdn. *IEEE Journal on Selected Areas in Communications*, 36(10):2358–2372, 2018.

[ds173] Kübra Kalkan, Gürkan Gür, and Fatih Alagöz. Sdnscore: A statistical defense mechanism against ddos attacks in sdn environment. In *2017 IEEE Symposium on Computers and Communications (ISCC)*, pages 669–675. IEEE, 2017.

[ds174] BV Karan, DG Narayan, and PS Hiremath. Detection of ddos attacks in software defined networks. In *2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS)*, pages 265–270. IEEE, 2018.

[ds175] Kallol Krishna Karmakar, Vijay Varadharajan, Surya Nepal, and Uday Tupakula. Sdn enabled secure iot architecture. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 581–585, 2019.

[ds176] Kallol Krishna Karmakar, Vijay Varadharajan, Surya Nepal, and Uday Tupakula. Sdn-enabled secure iot architecture. *IEEE Internet of Things Journal*, 8(8):6549–6564, 2020.

[ds177] Kallol Krishna Karmakar, Vijay Varadharajan, Uday Tupakula, and Michael Hitchens. Towards a dynamic policy enhanced integrated security architecture for sdn infrastructure. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–9. IEEE, 2020.

[ds178] Sanmeet Kaur and Maninder Singh. Hybrid intrusion detection and signature generation using deep recurrent neural networks. *Neural Computing and Applications*, 32:7859–7877, 2020.

[ds179] R Kesavamoorthy and K Ruba Soundar. Swarm intelligence based autonomous ddos attack detection and defense using multi agent system. *Cluster Computing*, 22(Suppl 4):9469–9476, 2019.

[ds180] G. Chenna Kesavulu. Preventing ddos attacks in software defined networks. In *2021 2nd International Conference on Range Technology (ICORT)*, pages 1–4, 2021.

[ds181] Samer Khamaiseh, Edoardo Serra, and Dianxiang Xu. vswitchguard: Defending openflow switches against saturation attacks. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 851–860. IEEE, 2020.

[ds182] Fatima Khashab, Joanna Moubarak, Antoine Feghali, and Carole Bassil. Ddos attack detection and mitigation in sdn using machine learning. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, pages 395–401. IEEE, 2021.

[ds183] Rinat Khayretdinov, Damir Dautov, Alexey Vulfin, Konstantin Mironov, and Arkadij Frid. Secure data exchange system in software-defined networks of energy complex facilities. In *2021 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, pages 58–63, 2021.

[ds184] Fakhry Khellah. Control plane packet-in arrival rate analysis for denial-of-service saturation attacks detection and mitigation in software-defined networks. *Arabian Journal for Science and Engineering*, 44(11):9349–9362, 2019.

[ds185] Yadav Ashok Khimabhai and Vandana Rohokale. Sdn control plane security in cloud computing against ddos attack. In *Proceedings of the International Conference on Advances in Information Communication Technology and Computing*, pages 1–5. ACM, 2016.

[ds186] Green Kim, Junghyun An, and Keecheon Kim. A study on authentication mechanism in seaas for sdn. In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, pages 1–6. ACM, 2017.

[ds187] Jinwoo Kim, Jaehyun Nam, Suyeol Lee, Vinod Yegneswaran, Phillip Porras, and Seungwon Shin. Bottlenet: Hiding network bottlenecks using sdn-based topology deception. *IEEE Transactions on Information Forensics and Security*, 16:3138–3153, 2021.

[ds188] Sangjun Kim, Yongsoon Eun, and Kyung-Joon Park. Stealthy sensor attack detection and real-time performance recovery for resilient cps. *IEEE Transactions on Industrial Informatics*, 17(11):7412–7422, 2021.

[ds189] Sunghwan Kim, Seunghyun Yoon, and Hyuk Lim. Deep reinforcement learning-based traffic sampling for multiple traffic analyzers on software-defined networks. *IEEE Access*, 9:47815–47827, 2021.

[ds190] Ili Ko, Desmond Chambers, and Enda Barrett. Feature dynamic deep learning approach for ddos mitigation within the isp domain. *International Journal of Information Security*, 19:53–70, 2020.

[ds191] Ralph Koning, Ben de Graaff, Gleb Polevoy, R Meijer, C de Laat, and Paola Grosso. Measuring the efficiency of sdn mitigations against attacks on computer infrastructures. *Future Generation Computer Systems*, 91:144–156, 2019.

[ds192] Heena Kousar, Mohammed Moin Mulla, Pooja Shettar, and DG Narayan. Detection of ddos attacks in software defined network using decision tree. In *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, pages 783–788. IEEE, 2021.

[ds193] Diego Kreutz, Jiangshan Yu, Fernando MV Ramos, and Paulo Esteves-Verissimo. Anchor: Logically centralized security for software-defined networks. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):1–36, 2019.

[ds194] Prabhakar Krishnan, Subhasri Duttagupta, and Krishnashree Achuthan. Sdnfv based threat monitoring and security framework for multi-access edge computing infrastructure. *Mobile Networks and Applications*, 24:1896–1923, 2019.

[ds195] Prabhakar Krishnan, Subhasri Duttagupta, and Krishnashree Achuthan. Varman: Multi-plane security framework for software defined networks. *Computer Communications*, 148:215–239, 2019.

[ds196] Prabhakar Krishnan, Subhasri Duttagupta, and Krishnashree Achuthan. Sdn/nfv security framework for fog-to-things computing infrastructure. *Software: Practice and Experience*, 50(5):757–800, 2020.

[ds197] Prabhakar Krishnan, Kurunandan Jain, Rajkumar Buyya, Pandi Vijayakumar, Anand Nayyar, Muhammad Bilal, and Houbing Song. Mud-based behavioral profiling security framework for software-defined iot networks. *IEEE Internet of Things Journal*, 2021.

[ds198] Chaitanya Kumar, Bathini Pranay Kumar, Aditya Chaudhary, Ayush Gupta, Kapil Dev, Ayushi Sharma, Shashank Srivastava, and B Rajitha. Intelligent ddos detection system in software-defined networking (sdn). In *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pages 1–6. IEEE, 2020.

[ds199] Shivansh Kumar and Ruhul Amin. Mitigating distributed denial of service attack: Blockchain and software-defined networking based approach, network model with future research challenges. *SECURITY AND PRIVACY*, 4(4):e163, 2021.

[ds200] Sourav Kunal, Parth Gandhi, Ronak Sutariya, and Hardik Tarpara. A secure software defined networking for distributed environment. *Security and Privacy*, page e130, 2020.

[ds201] Mochamad Teguh Kurniawan and Setiadi Yazid. A systematic literature review of security software defined network: research trends, threat, attack, detect, mitigate, and countermeasure. In *Proceedings of the 3rd International Conference on Telecommunications and Communication Engineering*, pages 39–45. ACM, 2019.

[ds202] Jonghoon Kwon, Dongwon Seo, Minjin Kwon, Heejo Lee, Adrian Perrig, and Hyogon Kim. An incrementally deployable anti-spoofing mechanism for software-defined networks. *Computer Communications*, 64:1–20, 2015.

[ds203] KC Lalropuia and Vandana Khaitan. Availability and reliability analysis of cloud computing under economic denial of sustainability (edos) attack: a semi-markov approach. *Cluster Computing*, 24:2177–2191, 2021.

[ds204] An Le, Phuong Dinh, Hoa Le, and Ngoc Cuong Tran. Flexible network-based intrusion detection and prevention system on software-defined networks. In *2015 International Conference on Advanced Computing and Applications (ACOMP)*, pages 106–111. IEEE, 2015.

[ds205] Tsung-Han Lee, Lin-Huang Chang, and Chao-Wei Syu. Deep learning enabled intrusion detection and prevention system over sdn networks. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2020.

[ds206] Cheng Lei, Hong-qi Zhang, Duo-he Ma, and Ying-jie Yang. Network moving target defense technique based on self-adaptive end-point hopping. *Arabian Journal for Science and Engineering*, 42(8):3249–3262, 2017.

[ds207] Chenxi Li, Jia Li, Jiahai Yang, and Jinlei Lin. A novel workload scheduling framework for intrusion detection system in nfv scenario. *Computers and Security*, 106:102271, 2021.

[ds208] Chuanhuang Li, Yan Wu, Xiaoyong Yuan, Zhengjun Sun, Weiming Wang, Xiaolin Li, and Liang Gong. Detection and defense of ddos attack–based on deep learning in openflow-based sdn. *International Journal of Communication Systems*, 31(5):e3497, 2018.

[ds209] Hongda Li, Feng Wei, and Hongxin Hu. Enabling dynamic network access control with anomaly-based ids and sdn. In *Proceedings of the ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization*, pages 13–16, 2019.

[ds210] Ruidong Li, Minjiao Zheng, Donglin Bai, and Zhengduo Chen. Sdn based intelligent honeynet network model design and verification. In *2021 International Conference on Machine Learning and Intelligent Systems Engineering (MLISE)*, pages 59–64, 2021.

[ds211] Wenjuan Li, Yu Wang, Zhiping Jin, Keping Yu, Jin Li, and Yang Xiang. Challenge-based collaborative intrusion detection in software-defined networking: An evaluation. *Digital Communications and Networks*, 2020.

[ds212] Xinmeng Li, Nengguang Luo, Dan Tang, Zhiqing Zheng, Zheng Qin, and Xinxiang Gao. Ba-bnn: Detect ldos attacks in sdn based on bat algorithm and bp neural network. In *2021 IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social Computing and Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pages 300–307. IEEE, 2021.

[ds213] Yang Li, Zhi-Ping Cai, and Hong Xu. Llmp: exploiting lldp for latency measurement in software-defined data center networks. *Journal of Computer Science and Technology*, 33:277–285, 2018.

[ds214] Jing Liu, Yingxu Lai, and Shixuan Zhang. Fl-guard: A detection and defense system for ddos attack in sdn. In *Proceedings of the 2017 international conference on cryptography, security and privacy*, pages 107–111. ACM, 2017.

[ds215] Qi Liu, Hongwei Ruan, Hua Li, Xiaodi Li, and Xianrong Wang. Real-guard: A machine learning based real-time mechanism for combining packet and flow features to mitigating network attacks in sdn. In *Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies*, CIAT 2020, page 451–458, New York, NY, USA, 2020. Association for Computing Machinery.

[ds216] Xing Liu. Towards blockchain-based resource allocation models for cloud-edge computing in iot applications. *Wireless Personal Communications*, pages 1–19, 2021.

[ds217] Ying Liu, Ting Zhi, Ming Shen, Lu Wang, Yikun Li, and Ming Wan. Software-defined ddos detection with information entropy analysis and optimized deep learning. *Future Generation Computer Systems*, 129:99–114, 2022.

[ds218] Zhenpeng Liu, Yupeng He, Wensheng Wang, Shuo Wang, Xiaofei Li, and Bin Zhang. Aeh-mtd: Adaptive moving target defense scheme for sdn. In *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 142–147. IEEE, 2019.

[ds219] Martin Andreoni Lopez, Diogo Menezes Ferrazani Mattos, and Otto Carlos MB Duarte. An elastic intrusion detection system for software networks. *Annals of Telecommunications*, 71(11-12):595–605, 2016.

[ds220] Yiqin Lu and Meng Wang. An easy defense mechanism against botnet-based ddos flooding attack originated in sdn environment using sflow. In *Proceedings of the 11th International Conference on Future Internet Technologies*, pages 14–20. ACM, 2016.

[ds221] Shibo Luo, Jun Wu, Jianhua Li, and Bei Pei. A defense mechanism for distributed denial of service attack in software-defined networks. In *2015 Ninth International Conference on Frontier of Computer Science and Technology*, pages 325–329. IEEE, 2015.

[ds222] Ricardo Macedo, Rafael de Castro, Aldri Santos, Yacine Ghamri-Doudane, and Michele Nogueira. Self-organized sdn controller cluster conformations against ddos attacks effects. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[ds223] Sebastián Gómez Macías, Luciano Paschoal Gaspary, and Juan Felipe Botero. Oracle: An architecture for collaboration of data and control planes to detect ddos attacks. *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 962–967, 2021.

[ds224] Jeevan Surya Maddu, Somanath Tripathy, and Sanjeet Kumar Nayak. Sdnguard: An extension in software defined network to defend dos attack. In *2019 IEEE Region 10 Symposium (TENSYMP)*, pages 44–49. IEEE, 2019.

[ds225] Surya Naryan Mahapatra, Binod Kumar Singh, and Vinay Kumar. A survey on secure transmission in internet of things: taxonomy, recent techniques, research requirements, and challenges. *Arabian Journal for Science and Engineering*, 45:6211–6240, 2020.

[ds226] Prasenjit Maity, Sandeep Saxena, Shashank Srivastava, Kshira Sagar Sahoo, Ashok Kumar Pradhan, and Neeraj Kumar. An effective probabilistic technique for ddos detection in openflow controller. *IEEE Systems Journal*, 2021.

[ds227] Jahanzaib Malik, Adnan Akhunzada, Iram Bibi, Muhammad Imran, Arslan Musaddiq, and Sung Won Kim. Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in sdn. *IEEE Access*, 8:134695–134706, 2020.

[ds228] Santosh Mani and Manisha J Nene. Preventing distributed denial of service attacks in software defined mesh networks. In *2021 International Conference on Intelligent Technologies (CONIT)*, pages 1–7, 2021.

[ds229] Santosh Mani and Manisha J Nene. Self-organizing software defined mesh networks to counter failures and attacks. In *2021 International Conference on Intelligent Technologies (CONIT)*, pages 1–7, 2021.

[ds230] Christopher Mansour and Danai Chasaki. Adaptive security monitoring for next-generation routers. *EURASIP Journal on Embedded Systems*, 2019(1):1–16, 2019.

[ds231] Eduard Marin, Nicola Bucciol, and Mauro Conti. An in-depth look into sdn topology discovery mechanisms: Novel attacks and practical countermeasures. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1101–1114, 2019.

[ds232] Rahim Masoudi and Ali Ghaffari. Software defined networks: A survey. *Journal of Network and computer Applications*, 67:1–25, 2016.

[ds233] Noman Mazhar, Rosli Salleh, Muhammad Zeeshan, M. Muzaffar Hameed, and Nauman Khan. R-idps: Real time sdn based idps system for iot security. In *2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, pages 71–76, 2021.

[ds234] Cristóbal Medina-López, Leocadio González Casado, Vicente González-Ruiz, and Yuansong Qiao. An sdn approach to detect targeted attacks in p2p fully connected overlays. *International Journal of Information Security*, 20:245–255, 2021.

[ds235] Roland Meier, David Gugelmann, and Laurent Vanbever. itap: In-network traffic analysis prevention using software-defined networks. In *Proceedings of the Symposium on SDN Research*, pages 102–114. ACM, 2017.

[ds236] Andrea Melis, Davide Berardi, Chiara Contoli, Franco Callegati, Flavio Esposito, and Marco Prandini. A policy checker approach for secure industrial sdn. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–7. IEEE, 2018.

[ds237] Júlio Mendonça, Jin-Hee Cho, Terrence J Moore, Frederica F Nelson, Hyuk Lim, Armin Zimmermann, and Dong Seong Kim. Performability analysis of services in a software-defined networking adopting time-based moving target defense mechanisms. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 1180–1189, 2020.

[ds238] Qinglan Meng, Xiyu Pang, Yanli Zheng, Gangwu Jiang, and Xin Tian. Development and optimization of software defined networking anomaly detection architecture by gru-cnn under deep learning. In *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*, pages 828–834. IEEE, 2021.

[ds239] Weizhi Meng, Wenjuan Li, Laurence T Yang, and Peng Li. Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. *International Journal of Information Security*, 19:279–290, 2020.

[ds240] Weizhi Meng, Wenjuan Li, and Jianying Zhou. Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration. *Information Fusion*, 70:60–71, 2021.

[ds241] Sugandhi Midha and Khushboo Triptahi. Extended tls security and defensive algorithm in openflow sdn. In *2019 9th International Conference on Cloud Computing, Data Science and Engineering (Confluence)*, pages 141–146. IEEE, 2019.

[ds242] Anupama Mishra, Brij B Gupta, Dragan Peraković, Shingo Yamaguchi, and Ching-Hsien Hsu. Entropy based defensive mechanism against ddos attack in sdn-cloud enabled online social networks. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6. IEEE, 2021.

[ds243] Anupama Mishra, Neena Gupta, and BB Gupta. Defense mechanisms against ddos attack based on entropy in sdn-cloud using pox controller. *Telecommunication systems*, 77:47–62, 2021.

[ds244] Reza Mohammadi, Mauro Conti, Chhagan Lal, and Satish C Kulhari. Syn-guard: An effective counter for syn flooding attack in software-defined networking. *International Journal of Communication Systems*, 32(17):e4061, 2019.

[ds245] Saif Saad Mohammed, Rasheed Hussain, Oleg Senko, Bagdat Bimaganbetov, JooYoung Lee, Fatima Hussain, Chaker Abdelaziz Kerrache, Ezedin Barka, and Md Zakirul Alam Bhuiyan. A new machine learning-based collaborative ddos mitigation mechanism in software-defined network. In *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–8. IEEE, 2018.

[ds246] Mehrnoosh Monshizadeh, Vikramajeet Khatri, and Raimo Kantola. Detection as a service: an sdn application. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pages 285–290. IEEE, 2017.

[ds247] Seyed Mohammad Mousavi and Marc St-Hilaire. Early detection of ddos attacks against software defined network controllers. *Journal of Network and Systems Management*, 26:573–591, 2018.

[ds248] Farha Akhter Munmun and Mahuwa Paul. Challenges of ddos attack mitigation in iot devices by software defined networking (sdn). In *2021 International Conference on Science and Contemporary Technologies (ICSCT)*, pages 1–5. IEEE, 2021.

[ds249] Hanan Mustapha and Ahmed M Alghamdi. Ddos attacks on the internet of things and their prevention methods. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, pages 1–5. ACM, 2018.

[ds250] Francesco Musumeci, Ali Can Fidanci, Francesco Paolucci, Filippo Cugini, and Massimo Tornatore. Machine-learning-enabled ddos attacks detection in p4 programmable networks. *Journal of Network and Systems Management*, 30:1–27, 2022.

[ds251] Hamza Mutaher and Pradeep Kumar. Security-enhanced sdn controller based kerberos authentication protocol. In *2021 11th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, pages 672–677, 2021.

[ds252] Keerthiraj Nagaraj, Allen Starke, and Janise McNair. Glass: A graph learning approach for software defined network based smart grid ddos security. In *ICC 2021-IEEE International Conference on Communications*, pages 1–6. IEEE, 2021.

[ds253] R Nagarathna and S Mercy Shalinie. Slamhha: A supervised learning approach to mitigate host location hijacking attack on sdn controllers. In *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, pages 1–7. IEEE, 2017.

[ds254] Tran Manh Nam, Phan Hai Phong, Tran Dinh Khoa, Truong Thu Huong, Pham Ngoc Nam, Nguyen Huu Thanh, Luong Xuan Thang, Pham Anh Tuan, Vu Duy Loi, et al. Self-organizing map-based approaches in ddos flooding detection using sdn. In *2018 International Conference on Information Networking (ICOIN)*, pages 249–254. IEEE, 2018.

[ds255] Niranjhana Narayanan, Ganesh C Sankaran, and Krishna M Sivalingam. Mitigation of security attacks in the sdn data plane using p4-enabled switches. In *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6. IEEE, 2019.

[ds256] Carlos Natalino, Carlos Manso, Ricard Vilalta, Paolo Monti, Raul Munõz, and Marija Furdek. Scalable physical layer security components for microservice-based optical sdn controllers. In *2021 European Conference on Optical Communication (ECOC)*, pages 1–4, 2021.

[ds257] Wajahat Navid and Muhammad Nasir Mumtaz Bhutta. Detection and mitigation of denial of service (dos) attacks using performance aware software defined networking (sdn). In *2017 International Conference on Information and Communication Technologies (ICICT)*, pages 47–57. IEEE, 2017.

[ds258] Ajay Nehra, Meenakshi Tripathi, Manoj Singh Gaur, Ramesh Babu Battula, and Chhagan Lal. Tilak: A token-based prevention approach for topology discovery threats in sdn. *International Journal of Communication Systems*, 32(17):e3781, 2019.

[ds259] Helio N Cunha Neto, Martin Andreoni Lopez, Natalia C Fernandes, and Diogo MF Mattos. Minecap: super incremental learning for detecting and blocking cryptocurrency mining on software-defined networking. *Annals of Telecommunications*, 75:121–131, 2020.

[ds260] Charles V Neu, Cássio G Tatsch, Roben C Lunardi, Regio A Michelin, Alex MS Orozco, and Avelino F Zorzo. Lightweight ips for port scan in openflow sdn networks. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6. IEEE, 2018.

[ds261] Charles V Neu, Avelino F Zorzo, Alex MS Orozco, and Regio A Michelin. An approach for detecting encrypted insider attacks on openflow sdn networks. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 210–215. IEEE, 2016.

[ds262] Hai Hoang Nguyen, Tri Gia Nguyen, Dinh Thai Hoang, Duc Tran Le, and Trung V Phan. Cars: Dynamic cyber-attack reaction in sdn-based networks with q-learning. In *2021 International Conference on Advanced Technologies for Communications (ATC)*, pages 156–161. IEEE, 2021.

[ds263] Hai Nam Nguyen, Hai Anh Tran, Scott Fowler, and Sami Souihi. A survey of blockchain technologies applied to software-defined networking: Research challenges and solutions. *IET Wireless Sensor Systems*, 2021.

[ds264] Tuan Anh Nguyen, Minjune Kim, Jangse Lee, Dugki Min, Jae-Woo Lee, and Dongseong Kim. Performability evaluation of switch-over moving target defence mechanisms in a software defined networking using stochastic reward nets. *Journal of Network and Computer Applications*, 199:103267, 2022.

[ds265] Jiseong Noh, Seunghyeon Lee, Jaehyun Park, Seungwon Shin, and Brent Byunghoon Kang. Vulnerabilities of network os and mitigation with state-based permission system. *Security and Communication Networks*, 9(13):1971–1982, 2016.

[ds266] Sichul Kevin Noh, Minjae Kang, and Minho Park. Protection against flow table overflow attack in software defined networks. In *2021 International Conference on Information Networking (ICOIN)*, pages 486–490, 2021.

[ds267] Matheus P Novaes, Luiz F Carvalho, Jaime Lloret, and Mario Lemes Proença. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access*, 8:83765–83781, 2020.

[ds268] Beny Nugraha, Naina Kulkarni, and Akash Gopikrishnan. Detecting adversarial ddos attacks in software-defined networking using deep learning techniques and adversarial training. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 448–454. IEEE, 2021.

[ds269] Heru Nurwarsito and Muhammad Fahmy Nadhif. Ddos attack early detection and mitigation system on sdn using random forest algorithm and ryu framework. In *2021 8th International Conference on Computer and Communication Engineering (ICCCE)*, pages 178–183. IEEE, 2021.

[ds270] Satoshi Okada, Yoshiki Fujiwara, Mariko Fujimoto, Wataru Matsuda, and Takuho Mitsunaga. Efficient incident response system on shared cyber threat information using sdn and stix. In *2021 IEEE International Conference on Computing (ICOCO)*, pages 109–114. IEEE, 2021.

[ds271] Prajakta M Ombase, Nayana P Kulkarni, Sudhir T Bagade, and Amrapali V Mhaisgawali. Dos attack mitigation using rule based and anomaly based techniques in software defined networking. In *2017 International Conference on Inventive Computing and Informatics (ICICI)*, pages 469–475. IEEE, 2017.

[ds272] Daichi Ono, Luis Guillen, Satoru Izumi, Toru Abe, and Takuo Suganuma. A proposal of port scan detection method based on packet-in messages in openflow networks and its evaluation. *International Journal of Network Management*, 31(6):e2174, 2021.

[ds273] Hitesh Padekar, Younghee Park, Hongxin Hu, and Sang-Yoon Chang. Enabling dynamic access control for controller applications in software-defined networks. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*, pages 51–61, 2016.

[ds274] Nicolae Paladi and Christian Gehrmann. Sdn access control for the masses. *Computers and Security*, 80:155–172, 2019.

[ds275] Xiang Pan, Vinod Yegneswaran, Yan Chen, Phillip Porras, and Seungwon Shin. Hogmap: Using sdns to incentivize collaborative security monitoring. In *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization*, pages 7–12, 2016.

[ds276] Taejune Park, Yeonkeun Kim, and Seungwon Shin. Unisafe: A union of security actions for software switches. In *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization*, pages 13–18, 2016.

[ds277] Younghee Park, Nikhil Vijayakumar Kengalahalli, and Sang-Yoon Chang. Distributed security network functions against botnet attacks in software-defined networks. In *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–7. IEEE, 2018.

[ds278] Túlio A Pascoal, Iguatemi E Fonseca, and Vivek Nigam. Slow denial-of-service attacks on software defined networks. *Computer Networks*, page 107223, 2020.

[ds279] Achilleas Pasias, Thanasis Kotsiopoulos, Georgios Lazaridis, Anastasios Drosou, Dimitrios Tzovaras, and Panagiotis Sarigiannidis. Enabling cyber-attack mitigation techniques in a software defined network. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 497–502. IEEE, 2021.

[ds280] Shivam Patidar and Samayveer Singh. Information theory-based techniques to detect ddos in sdn: A survey. In *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, pages 529–534. IEEE, 2021.

[ds281] Naina Patrascu, Alina Dartu, Tudor Cornea, Serban Georgica Obreja, Marina Ciurezu, and Alexandru Brumaru. Security solution for cloud based on software defined networking. In *2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pages 1–6, 2021.

[ds282] Aditya Patwardhan, Deepthi Jayarama, Nitish Limaye, Shivaji Vidhale, Zarna Parekh, and Khaled Harfoush. Sdn security: Information disclosure and flow table overflow attacks. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[ds283] Nikolaos E Petroulakis, Konstantinos Fysarakis, Ioannis Askoxylakis, and George Spanoudakis. Reactive security for sdn/nfv-enabled industrial networks leveraging service function chaining. *Transactions on Emerging Telecommunications Technologies*, 29(7):e3269, 2018.

[ds284] Trung V Phan, Nguyen Khac Bao, and Minho Park. Distributed-som: A novel performance bottleneck handler for large-sized software-defined networks under flooding attacks. *Journal of Network and Computer Applications*, 91:14–25, 2017.

[ds285] Trung V Phan, Tri Gia Nguyen, Nhu-Ngoc Dao, Truong Thu Huong, Nguyen Huu Thanh, and Thomas Bauschert. Deepguard: Efficient anomaly detection in sdn with fine-grained traffic flow monitoring. *IEEE Transactions on Network and Service Management*, 17(3):1349–1362, 2020.

[ds286] Andrés Felipe Murillo Piedrahita, Sandra Rueda, Diogo MF Mattos, and Otto Carlos MB Duarte. Flowfence: a denial of service defense system for software defined networking. In *2015 Global Information Infrastructure and Networking Symposium (GIIS)*, pages 1–6. IEEE, 2015.

[ds287] Harikrishna Pillutla and Amuthan Arjunan. Fuzzy self organizing maps-based ddos mitigation mechanism for software defined networking in cloud computing. *Journal of Ambient Intelligence and Humanized Computing*, 10:1547–1559, 2019.

[ds288] Huseyin Polat, Muammer Turkoglu, and Onur Polat. Deep network approach with stacked sparse autoencoders in detection of ddos attacks on sdn-based vanet. *IET Communications*, 14(22):4089–4100, 2021.

[ds289] Aayush Pradhan and Rejo Mathew. Solutions to vulnerabilities and threats in software defined networking (sdn). *Procedia Computer Science*, 171:2581–2589, 2020.

[ds290] Aditya Prakash and Rojalina Priyadarshini. An intelligent software defined network controller for preventing distributed denial of service attack. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pages 585–589. IEEE, 2018.

[ds291] Mahesh Kumar Prasath and Balasubramani Perumal. A meta-heuristic bayesian network classification for intrusion detection. *International Journal of Network Management*, 29(3):e2047, 2019.

[ds292] Rifqi Fauzan Pratama, Novian Anggis Suwastika, and Muhammad Arief Nugroho. Design and implementation adaptive intrusion prevention system (ips) for attack prevention in software-defined network (sdn) architecture. In *2018 6th International Conference on Information and Communication Technology (ICoICT)*, pages 299–304. IEEE, 2018.

[ds293] Rojalina Priyadarshini, Rabindra Kumar Barik, and Harishchandra Dubey. Fog-sdn: A light mitigation scheme for ddos attack in fog computing framework. *International Journal of Communication Systems*, 33(9):e4389, 2020.

[ds294] Karthik Raghunath and Prabhakar Krishnan. Towards a secure sdn architecture. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2018.

[ds295] Obaid Rahman, Mohammad Ali Gauhar Quraishi, and Chung-Horng Lung. Ddos attacks detection and mitigation in sdn using machine learning. In *2019 IEEE World Congress on Services (SERVICES)*, volume 2642, pages 184–189. IEEE, 2019.

[ds296] Mohamed Rahouti, Kaiqi Xiong, Nasir Ghani, and Farooq Shaikh. Synguard: Dynamic threshold-based syn flood attack detection and mitigation in software-defined networks. *IET Networks*, 10(2):76–87, 2021.

[ds297] J Ramprasath and V Seethalakshmi. Improved network monitoring using software-defined networking for ddos detection and mitigation evaluation. *Wireless Personal Communications*, 116(3):2743–2757, 2021.

[ds298] Stefan Rass, Benjamin Rainer, Matthias Vavti, Johannes Göllner, Andreas Peer, and Stefan Schauer. Secure communication over software-defined networks. In *Internet of Things. IoT Infrastructures: First International Summit, IoT360 2014, Rome, Italy, October 27-28, 2014, Revised Selected Papers, Part II 1*, pages 211–221. Springer, 2015.

[ds299] Bilal Rauf, Haider Abbas, Muhammad Usman, Tanveer A. Zia, Waseem Iqbal, Yawar Abbas, and Hammad Afzal. Application threats to exploit northbound interface vulnerabilities in software defined networks. *ACM Computing Surveys*, 54(6):1–36, 2021. Publisher Copyright: © 2021 ACM.

[ds300] Nagarathna Ravi and S Mercy Shalinie. Blacknurse-sc: A novel attack on sdn controller. *IEEE Communications Letters*, 25(7):2146–2150, 2021.

[ds301] Filippo Rebecchi, Julien Boite, Pierre-Alexis Nardin, Mathieu Bouet, and Vania Conan. Ddos protection with stateful software-defined networking. *International Journal of Network Management*, 29(1):e2042, 2019.

[ds302] Admilson de Ribamar Lima Ribeiro, Reneilson Yves Carvalho Santos, and Anderson Clayton Alves Nascimento. Anomaly detection technique for intrusion detection in sdn environment using continuous data stream machine learning algorithms. In *2021 IEEE International Systems Conference (SysCon)*, pages 1–7. IEEE, 2021.

[ds303] Christian Röpke and Thorsten Holz. On network operating system security. *International Journal of Network Management*, 26(1):6–24, 2016.

[ds304] Chen Runze, Ruan Fangming, Li Yidan, Yin Lan, and Chen Yanli. A simple ddos defense method based sdn. In *2021 IEEE 15th International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, pages 88–92. IEEE, 2021.

[ds305] E.S. Sagatov, S. Mayhoub, A.M. Sukhov, F. Esposito, and P. Calyam. Proactive detection for countermeasures on port scanning based attacks. In *2021 17th International Conference on Network and Service Management (CNSM)*, pages 402–406, 2021.

[ds306] Rishikesh Sahay, Gregory Blanc, Zonghua Zhang, and Hervé Debar. Aroma: An sdn based autonomic ddos mitigation framework. *computers and security*, 70:482–499, 2017.

[ds307] Rishikesh Sahay, Gregory Blanc, Zonghua Zhang, Khalifa Toumi, and Hervé Debar. Adaptive policy-driven attack mitigation in sdn. In *Proceedings of the 1st International Workshop on Security and Dependability of Multi-Domain Infrastructures*, pages 1–6. ACM, 2017.

[ds308] Rishikesh Sahay, Weizhi Meng, and Christian D Jensen. The application of software defined networking on securing computer networks: A survey. *Journal of Network and Computer Applications*, 131:89–108, 2019.

[ds309] Kshira Sagar Sahoo, Amaan Iqbal, Prasenjit Maiti, and Bibhudatta Sahoo. A machine learning approach for predicting ddos traffic in software defined networks. In *2018 International Conference on Information Technology (ICIT)*, pages 199–203. IEEE, 2018.

[ds310] Kshira Sagar Sahoo, Sanjaya Kumar Panda, Sampa Sahoo, Bibhudatta Sahoo, and Ratnakar Dash. Toward secure software-defined networks against distributed denial of service attack. *The Journal of Supercomputing*, 75:4829–4874, 2019.

[ds311] Kshira Sagar Sahoo and Deepak Puthal. Sdn-assisted ddos defense framework for the internet of multimedia things. *ACM Trans. Multimedia Comput. Commun. Appl.*, 16(3s), 2020.

[ds312] Kshira Sagar Sahoo, Deepak Puthal, Mayank Tiwary, Joel JPC Rodrigues, Bibhudatta Sahoo, and Ratnakar Dash. An early detection of low rate ddos attack to sdn based data center networks using information distance metrics. *Future Generation Computer Systems*, 89:685–697, 2018.

[ds313] Luis E Salazar and Alvaro A Cardenas. Enhancing the resiliency of cyber-physical systems with software-defined networks. In *Proceedings of the ACM Workshop on Cyber-Physical Systems Security and Privacy*, pages 15–26, 2019.

[ds314] A Samson and NP Gopalan. Software defined networking: Identification of pathways for security threats. In *Proceedings of the International Conference on Informatics and Analytics*, pages 1–6. ACM, 2016.

[ds315] Hunor Sándor, Béla Genge, Zoltán Szántó, Lőrinc Márton, and Piroska Haller. Cyber attack detection and mitigation: Software defined survivable industrial control systems. *International Journal of Critical Infrastructure Protection*, 25:152–168, 2019.

[ds316] Abimbola Sangodoyin, Babagana Modu, Irfan Awan, and Jules Pagna Disso. An approach to detecting distributed denial of service attacks in software defined networks. In *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 436–443. IEEE, 2018.

[ds317] Abimbola O Sangodoyin, Mobayode O Akinsolu, Prashant Pillai, and Vic Grout. Detection and classification of ddos flooding attacks on software-defined networks: A case study for the application of machine learning. *IEEE Access*, 9:122495–122508, 2021.

[ds318] Dorabella Santos, Amaro De Sousa, Carmen Mas-Machuca, and Jacek Rak. Assessment of connectivity-based resilience to attacks against multiple nodes in sdns. *IEEE Access*, 9:58266–58286, 2021.

[ds319] A Sarkunavathi and V Srinivasan. A scrutinized study on dos attacks in wireless sensor networks and need of sdn in mitigating dos attacks. In *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–10. IEEE, 2021.

[ds320] Muhammad Arslan Sarwar, Majid Hussain, Muhammad Usman Anwar, and Mudassar Ahmad. Flowjustifier: An optimized trust-based request prioritization approach for mitigation of sdn controller ddos attacks in the iot paradigm. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pages 1–9. ACM, 2019.

[ds321] N Satheesh, MV Rathnamma, Assicate Professor G Rajeshkumar, P Vidya Sagar, Pankaj Dadheech, SR Dogiwal, Priya Velayutham, and Sudhakar Sengan. Flow-based anomaly intrusion detection using machine learning model with software defined networking for openflow network. *Microprocessors and Microsystems*, page 103285, 2020.

[ds322] Danish Sattar, Ashraf Matrawy, and Olufemi Adeojo. Adaptive bubble burst (abb): Mitigating ddos attacks in software-defined networks. In *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*, pages 50–55. IEEE, 2016.

[ds323] Gustavo F Scaranti, Luiz F Carvalho, Sylvio Barbon, and Mario Lemes Proença. Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks. *IEEE Access*, 2020.

[ds324] Gustavo Frigo Scaranti, Luiz Fernando Carvalho, Sylvio Barbon, Jaime Lloret, and Mario Lemes Proença. Unsupervised online anomaly detection in software defined network environments. *Expert Systems with Applications*, 191:116225, 2022.

[ds325] Sandra Scott-Hayward and Thianantha Arumugam. Ofmtl-sec: State-based security for software defined networks. In *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 1–7. IEEE, 2018.

[ds326] Anass Sebbar, ZKIK Karim, Youssef Baadi, Mohammed Boulmalf, and Mohamed Dâfir Ech-Cherif El Kettani. Using advanced detection and prevention technique to mitigate threats in sdn architecture. In *2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 90–95. IEEE, 2019.

[ds327] Anass Sebbar, Karim Zkik, Youssef Baddi, Mohammed Boulmalf, and Mohamed Dafir Ech-Cherif El Kettani. Mitm detection and defense mechanism cbna-rf based on machine learning for large-scale sdn context. *Journal of Ambient Intelligence and Humanized Computing*, 11:5875–5894, 2020.

[ds328] Gustavo A Nunez Segura, Arsenia Chorti, and Cintia Borges Margi. Centralized and distributed intrusion detection for resource-constrained wireless sdn networks. *IEEE Internet of Things Journal*, 2021.

[ds329] Gustavo A Nunez Segura, Arsenia Chorti, and Cintia Borges Margi. Distributed dos attack detection in sdn: Tradeoffs in resource constrained wireless networks. In *2021 IEEE Statistical Signal Processing Workshop (SSP)*, pages 131–135. IEEE, 2021.

[ds330] Lanka Chris Sejaphala and Mthulisi Velempini. The design of a defense mechanism to mitigate sinkhole attack in software defined wireless sensor cognitive radio networks. *Wireless Personal Communications*, 113:977–993, 2020.

[ds331] Letian Sha, Liwen He, Jianming Fu, Jing Sun, and Pengwei Li. Sdn-based sensitive information (si) protection: sensitivity-degree measurement in software and data lifetime supervisor in software defined network. *Security and Communication Networks*, 9(13):1944–1957, 2016.

[ds332] Arash Shaghaghi, Mohamed Ali Kaafar, and Sanjay Jha. Wedgetail: An intrusion prevention system for the data plane of software defined networks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 849–861. ACM, 2017.

[ds333] Sayed Qaiser Ali Shah, Farrukh Zeeshan Khan, and Muneer Ahmad. Mitigating tcp syn flooding based edos attack in cloud computing environment using binomial distribution in sdn. *Computer Communications*, 182:198–211, 2022.

[ds334] Alireza Shameli-Sendi, Makan Pourzandi, Mohamed Fekih-Ahmed, and Mohamed Cheriet. Taxonomy of distributed denial of service mitigation approaches for cloud computing. *Journal of Network and Computer Applications*, 58:165–179, 2015.

[ds335] Jia Shan-Shan and Xu Ya-Bin. The apt detection method in sdn. In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pages 1240–1245. IEEE, 2017.

[ds336] Jia Shan-Shan and Xu Ya-Bin. The apt detection method based on attack tree for sdn. In *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*, pages 116–121. ACM, 2018.

[ds337] Fengjun Shang, Yan Li, Qiang Fu, Wenkai Wang, Jiangfan Feng, and Li He. Distributed controllers multi-granularity security communication mechanism for software-defined networking. *Computers and Electrical Engineering*, 66:388–406, 2018.

[ds338] Harsh Sharma and Shashank Gupta. Leveraging machine learning and sdn-fog infrastructure to mitigate flood attacks. In *2021 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2021.

[ds339] Pradip Kumar Sharma, Jin Ho Park, Young-Sik Jeong, and Jong Hyuk Park. Shsec: sdn based secure smart home network architecture for internet of things. *Mobile Networks and Applications*, 24:913–924, 2019.

[ds340] Pradip Kumar Sharma, Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Communications Magazine*, 55(9):78–85, 2017.

[ds341] Khan Mohammad Shayshab Azad, Nayon Hossain, Md. Jahidul Islam, Anichur Rahman, and Sumaiya Kabir. Preventive determination and avoidance of ddos attack with sdn over the iot networks. In *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, pages 1–6, 2021.

[ds342] Congqi Shen, Geyang Xiao, Shaofeng Yao, Boyang Zhou, Zhongxia Pan, and Hong Zhang. An lstm based malicious traffic attack detection in industrial internet. In *2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, pages 60–65. IEEE, 2021.

[ds343] Jiahao Shen, Tao Zhang, Bingchi Zhang, Weixiao Ji, Xiaohui Kuang, and Changqiao Xu. Ppo-rm: Proximal policy optimization based route mutation for multimedia services. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pages 35–40, 2021.

[ds344] Yi Shen, Chunming Wu, Dezhang Kong, and Mingliang Yang. Tpdd: A two-phase ddos detection system in software-defined networking. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

[ds345] Zi-Yang Shen, Ming-Wei Su, Yun-Zhan Cai, and Meng-Hsun Tasi. Mitigating syn flooding and udp flooding in p4-based sdn. In *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pages 374–377. IEEE, 2021.

[ds346] Jiangyong Shi, Yingzhi Zeng, Wenhao Wang, and Yuexiang Yang. Feedback based sampling for intrusion detection in software defined network. In *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*, pages 95–99. ACM, 2018.

[ds347] Alireza Shirmarz, Ali Ghaffari, Ramin Mohammadi, and Sedat Akleylek. Ddos attack detection accuracy improvement in software defined network (sdn) using ensemble classification. In *2021 International Conference on Information Security and Cryptology (ISC-TURKEY)*, pages 111–115. IEEE, 2021.

[ds348] Reza Bakhtiari Shohani and Seyed Akbar Mostafavi. Introducing a new linear regression based method for early ddos attack detection in sdn. In *2020 6th International Conference on Web Research (ICWR)*, pages 126–132. IEEE, 2020.

[ds349] G Shravanya, NH Swati, Ram P Rustagi, and Oshin Sharma. Securing distributed sdn controller network from induced dos attacks. In *2019 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, pages 9–16. IEEE, 2019.

[ds350] Jiangang Shu, Lei Zhou, Weizhe Zhang, Xiaojiang Du, and Mohsen Guizani. Collaborative intrusion detection for vanets: a deep learning-based distributed sdn approach. *IEEE Transactions on Intelligent Transportation Systems*, 22(7):4519–4530, 2020.

[ds351] Jagdeep Singh and Sunny Behal. A novel approach for the detection of ddos attacks in sdn using information theory metric. In *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 512–516. IEEE, 2021.

[ds352] Maninder Pal Singh and Abhinav Bhandari. New-flow based ddos attacks in sdn: Taxonomy, rationales, and research challenges. *Computer Communications*, 2020.

[ds353] Maninderpal Singh, Gagangeet Singh Aujla, Amritpal Singh, Neeraj Kumar, and Sahil Garg. Deep-learning-based blockchain framework for secure software-defined industrial networks. *IEEE Transactions on Industrial Informatics*, 17(1):606–616, 2020.

[ds354] Sukhvinder Singh and SKV Jayakumar. A study on various attacks and detection methodologies in software defined networks. *Wireless Personal Communications*, 114(1):675–697, 2020.

[ds355] Mitali Sinha, Padmalochan Bera, and Manoranjan Satpathy. An anomaly free distributed firewall system for sdn. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–8. IEEE, 2021.

[ds356] Michael Sjoholmsierchio, Britta Hale, Daniel Lukaszewski, and Geoffrey Xie. Strengthening sdn security: Protocol dialecting and downgrade attacks. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, pages 321–329, 2021.

[ds357] Dylan Smyth, Donna O'Shea, Victor Cionca, and Sean McSweeney. Attacking distributed software-defined networks by leveraging network state consistency. *Computer Networks*, 156:9–19, 2019.

[ds358] Manish Snehi and Abhinav Bhandari. An sdn/nfv based intelligent fog architecture for ddos defense in cyber physical systems. In *2021 10th International Conference on System Modeling and Advancement in Research Trends (SMART)*, pages 229–234. IEEE, 2021.

[ds359] Sanaz Soltani, Mohammad Shojafar, Habib Mostafaei, Zahra Pooranian, and Rahim Tafazolli. Link latency attack in software-defined networks. In *2021 17th International Conference on Network and Service Management (CNSM)*, pages 187–193. IEEE, 2021.

[ds360] Yan Song, Wenjing Luo, Jian Li, Panfeng Xu, and Jianwei Wei. Sdn-based industrial internet security gateway. In *2021 International Conference on Security, Pattern Analysis, and Cybernetics(SPAC)*, pages 238–243, 2021.

[ds361] Mustafa Soylu, Luis Guillen, Satoru Izumi, Toru Abe, and Takuo Suganuma. Nfv-guard: Mitigating flow table-overflow attacks in sdn using nfv. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, pages 263–267. IEEE, 2021.

[ds362] Vignesh Sridharan and Mohan Gurusamy. Game-theoretic framework for malicious controller detection in software defined networks. *IEEE Transactions on Network and Service Management*, 18(3):3107–3120, 2021.

[ds363] Jinshu Su, Wen Wang, and Cong Liu. A survey of control consistency in software-defined networking. *CCF Transactions on Networking*, 2(3-4):137–152, 2019.

[ds364] K Muthamil Sudar, M Beulah, P Deepalakshmi, P Nagaraj, and P Chinnasamy. Detection of distributed denial of service attacks in sdn using machine learning techniques. In *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–5. IEEE, 2021.

[ds365] Bambang Susilo and Riri Fitri Sari. Intrusion detection in software defined network using deep learning approach. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0807–0812. IEEE, 2021.

[ds366] Rochak Swami, Mayank Dave, and Virender Ranga. Software-defined networking-based ddos defense mechanisms. *ACM Computing Surveys (CSUR)*, 52(2):1–36, 2019.

[ds367] Rochak Swami, Mayank Dave, and Virender Ranga. Voting-based intrusion detection framework for securing software-defined networks. *Concurrency and Computation: Practice and Experience*, page e5927, 2020.

[ds368] Rochak Swami, Mayank Dave, and Virender Ranga. Addressing spoofed ddos attacks in software-defined networking. In *2021 6th International Conference for Convergence in Technology (I2CT)*, pages 1–7, 2021.

[ds369] Rochak Swami, Mayank Dave, and Virender Ranga. Detection and analysis of tcp-syn ddos attack in software-defined networking. *Wireless Personal Communications*, 118:2295–2317, 2021.

[ds370] Ava Tahmasebi, Ahmad Salahi, and Mohammad Ali Pourmina. A novel feature-based ddos detection and mitigation scheme in sdn controller using queueing theory. *Wireless Personal Communications*, 117:1985–2006, 2021.

[ds371] Junyuan Tan, Shan Jing, Lei Guo, and Bin Xiao. Ddos detection method based on gini impurity and random forest in sdn environment. In *2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, pages 601–606. IEEE, 2021.

[ds372] D Tang, Siqi Zhang, Yudong Yan, Jingwen Chen, and Zheng Qin. Real-time detection and mitigation of ldos attacks in the sdn using the hgb-fp algorithm. *IEEE Transactions on Services Computing*, pages 1–1, 2021.

[ds373] Dan Tang, Yudong Yan, Siqi Zhang, Jingwen Chen, and Zheng Qin. Performance and features: Mitigating the low-rate tcp-targeted dos attack via sdn. *IEEE Journal on Selected Areas in Communications*, 40(1):428–444, 2022.

[ds374] Dan Tang, Dongshuo Zhang, Huan Zhao, Dashun Liu, Yudong Yan, and Jingwen Chen. Work in progress: Network attack detection towards smart factory. In *2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pages 485–488, 2021.

[ds375] Omer Elsier Tayfour and Muhammad Nadzir Marsono. Collaborative detection and mitigation of distributed denial-of-service attacks on software-defined network. *Mobile Networks and Applications*, 25:1338–1347, 2020.

[ds376] Omer Elsier Tayfour and Muhammad Nadzir Marsono. Collaborative detection and mitigation of ddos in software-defined networks. *The Journal of Supercomputing*, 77:13166–13190, 2021.

[ds377] Vianney Kengne Tchendji, Fabrice Mvah, Clémentin Tayou Djamegni, and Yannick Florian Yankam. E2basep: Efficient bayes based security protocol against arp spoofing attacks in sdn architectures. *Journal of Hardware and Systems Security*, 5:58–74, 2021.

[ds378] Kashyap Thimmaraju, Liron Schiff, and Stefan Schmid. Preacher: Network policy checker for adversarial environments. In *2019 38th Symposium on Reliable Distributed Systems (SRDS)*, pages 32–3209, 2019.

[ds379] Wen Tian, Miao Du, Xiaopeng Ji, Guangjie Liu, Yuewei Dai, and Zhu Han. Honeypot detection strategy against advanced persistent threats in industrial internet of things: a prospect theoretic game. *IEEE Internet of Things Journal*, 8(24):17372–17381, 2021.

[ds380] Yun Tian, Vincent Tran, and Mutalifu Kuerban. Dos attack mitigation strategies on sdn controller. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0701–0707. IEEE, 2019.

[ds381] Thuy Vinh Tran and Heejune Ahn. Challenges of and solution to the control load of stateful firewall in software defined networks. *Computer Standards and Interfaces*, 54:293–304, 2017.

[ds382] Bata Krishna Tripathy, Debi Prasad Das, Swagat Kumar Jena, and Padmalochan Bera. Risk based security enforcement in software defined network. *computers and security*, 78:321–335, 2018.

[ds383] Yuchia Tseng, Farid Naït-Abdesselam, and Ashfaq Khokhar. A comprehensive 3-dimensional security analysis of a controller in software-defined networking. *Security and Privacy*, 1(2):e21, 2018.

[ds384] Enkhtur Tsogbaatar, Monowar H Bhuyan, Yuzo Taenaka, Doudou Fall, Khishigjargal Gonchigsumlaa, Erik Elmroth, and Youki Kadobayashi. Del-iot: A deep ensemble learning approach to uncover anomalies in iot. *Internet of Things*, 14:100391, 2021.

[ds385] Taef Uddin Nadim and Foysal. Towards autonomic entropy based approach for ddos attack detection and mitigation using software defined networking. In *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, pages 1–5, 2021.

[ds386] Benjamin E Ujcich, Samuel Jero, Anne Edmundson, Qi Wang, Richard Skowyra, James Landry, Adam Bates, William H Sanders, Cristina Nita-Rotaru, and Hamed Okhravi. Cross-app poisoning in software-defined networking. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 648–663, 2018.

[ds387] Raja Majid Ali Ujjan, Zeeshan Pervez, and Keshav Dahal. Suspicious traffic detection in sdn with collaborative techniques of snort and deep neural networks. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 915–920. IEEE, 2018.

[ds388] Raja Majid Ali Ujjan, Zeeshan Pervez, and Keshav Dahal. Snort based collaborative intrusion detection system using blockchain in sdn. In *2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, pages 1–8. IEEE, 2019.

[ds389] Raja Majid Ali Ujjan, Zeeshan Pervez, Keshav Dahal, Ali Kashif Bashir, Rao Mumtaz, and J González. Towards sflow and adaptive polling sampling for deep learning based ddos detection in sdn. *Future Generation Computer Systems*, 111:763–779, 2020.

[ds390] Emre Unal, Sonali Sen-Baidya, and Rattikorn Hewett. Towards prediction of security attacks on software defined networks: A big data analytic approach. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 4582–4588. IEEE, 2018.

[ds391] Prakriti Vaid, Sudesh Kumar Bhadu, and Raj M Vaid. Intrusion detection system in software defined network using machine learning approach-survey. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, pages 803–807. IEEE, 2021.

[ds392] Nguyen Thanh Van, Ho Bao, and Tran Ngoc Thinh. An anomaly-based intrusion detection architecture integrated on openflow switch. In *Proceedings of the 6th International Conference on Communication and Network Security*, pages 99–103. ACM, 2016.

[ds393] Phan Van Trung, Truong Thu Huong, Dang Van Tuyen, Duong Minh Duc, Nguyen Huu Thanh, and Alan Marshall. A multi-criteria-based ddos-attack prevention solution using software defined networking. In *2015 International Conference on Advanced Technologies for Communications (ATC)*, pages 308–313. IEEE, 2015.

[ds394] Vijay Varadharajan, Uday Tupakula, and Kallol Karmakar. Software enabled security architecture and mechanisms for securing 5g network services, 2020.

[ds395] Josy Elsa Varghese and Balachandra Muniyal. An efficient ids framework for ddos attacks in sdn environment. *IEEE Access*, 9:69680–69699, 2021.

[ds396] Josy Elsa Varghese and Balachandra Muniyal. Trend in sdn architecture for ddos detection- a comparative study. In *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, pages 170–174, 2021.

[ds397] S Veena and R Manju. Detection and mitigation of security attacks using real time sdn analytics. In *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)*, volume 2, pages 87–93. IEEE, 2017.

[ds398] S Velliangiri and J Premalatha. Intrusion detection of distributed denial of service attack in cloud. *Cluster Computing*, 22(Suppl 5):10615–10623, 2019.

[ds399] P Velmurugadass, S Dhanasekaran, S Shasi Anand, and V Vasudevan. Enhancing blockchain security in cloud computing with iot environment using ecies and cryptography hash algorithm. *Materials Today: Proceedings*, 37:2653–2659, 2021.

[ds400] Varsha Venugopal, Jim Alves-Foss, and Sandeep Gogineni Ravindrababu. Use of an sdn switch in support of nist ics security recommendations and least privilege networking. In *Proceedings of the Fifth Annual Industrial Control System Security (ICSS) Workshop*, pages 11–20. ACSAC, 2019.

[ds401] Priyanka Verma, Shashikala Tapaswi, and W Wilfred Godfrey. A service governance and isolation based approach to mitigate internal collateral damages in cloud caused by ddos attack. *Wireless Networks*, 27:2529–2548, 2021.

[ds402] Alfredo Menezes Vieira, Rubens de Souza Matos Junior, and Admilson de Ribamar Lima Ribeiro. Systematic mapping on prevention of ddos attacks on software defined networks. In *2021 IEEE International Systems Conference (SysCon)*, pages 1–8, 2021.

[ds403] Haopei Wang, Lei Xu, and Guofei Gu. Floodguard: A dos attack prevention extension in software-defined networks. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 239–250. IEEE, 2015.

[ds404] Haopei Wang, Guangliang Yang, Phakpoom Chinprutthiwong, Lei Xu, Yangyong Zhang, and Guofei Gu. Towards fine-grained network security forensics and diagnosis in the sdn era. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16, 2018.

[ds405] Jiadai Wang and Jiajia Liu. Location hijacking attack in software-defined space-air-ground integrated vehicular network. *IEEE Internet of Things Journal*, 2021.

[ds406] Lei Wang, Qing Li, Yong Jiang, Xuya Jia, and Jianping Wu. Woodpecker: Detecting and mitigating link-flooding attacks via sdn. *Computer Networks*, 147:1–13, 2018.

[ds407] Lu Wang and Ying Liu. A ddos attack detection method based on information entropy and deep learning in sdn. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, volume 1, pages 1084–1088. IEEE, 2020.

[ds408] Meng Wang, Yiqin Lu, and Jiancheng Qin. Source-based defense against ddos attacks in sdn based on sflow and som. *IEEE Access*, 10:2097–2116, 2022.

[ds409] Puming Wang, Laurence T Yang, Xin Nie, Zhian Ren, Jintao Li, and Liwei Kuang. Data-driven software defined network attack detection: State-of-the-art and perspectives. *Information Sciences*, 513:65–83, 2020.

[ds410] Qian Wang, Zhifeng Zhao, and Honggang Zhang. Ddos defense mechanism based on software defined network. In *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, pages 1122–1127. IEEE, 2017.

[ds411] Shen Wang, Jun Wu, Wu Yang, and Long-hua Guo. Novel architectures and security solutions of programmable software-defined networking: a comprehensive survey. *Frontiers of Information Technology & Electronic Engineering*, 19(12):1500–1521, 2018.

[ds412] Song Wang, Karina Gomez Chavez, and Sithamparanathan Kandeepan. Seco: Sdn secure controller algorithm for detecting and defending denial of service attacks. In *2017 5th International Conference on Information and Communication Technology (ICoIC7)*, pages 1–6. IEEE, 2017.

[ds413] Tao Wang, Yaokai Feng, and Kouichi Sakurai. Improving the two-stage detection of cyberattacks in sdn environment using dynamic thresholding. In *2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, pages 1–7. IEEE, 2021.

[ds414] Wen Wang, Wenbo He, and Jinshu Su. Network intrusion detection and prevention middlebox management in sdn. In *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, pages 1–8. IEEE, 2015.

[ds415] Xiulei Wang, Ming Chen, and Changyou Xing. Sdsnm: a software-defined security networking mechanism to defend against ddos attacks. In *2015 Ninth International Conference on Frontier of Computer Science and Technology*, pages 115–121. IEEE, 2015.

[ds416] Yang Wang, Tao Hu, Guangming Tang, Jichao Xie, and Jie Lu. Sgs: Safe-guard scheme for protecting control plane against ddos attacks in software-defined networking. *IEEE Access*, 7:34699–34710, 2019.

[ds417] You-Chiun Wang and Yi-Chuan Wang. Efficient and low-cost defense against distributed denial-of-service attacks in sdn-based networks. *International Journal of Communication Systems*, 33(14):e4461, 2020.

[ds418] You-Chiun Wang and Ren-Xuan Ye. Credibility-based countermeasure against slow http dos attacks by using sdn. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0890–0895. IEEE, 2021.

[ds419] Yulong Wang, Qingyu Chen, Junjie Yi, and Jun Guo. U-tri: Unlinkability through random identifier for sdn network. In *Proceedings of the 2017 Workshop on Moving Target Defense*, pages 3–15. ACM, 2017.

[ds420] Azka Wani and S Revathi. Ddos detection and alleviation in iot using sdn (sdiot-ddos-da). *Journal of The Institution of Engineers (India): Series B*, 101(2):117–128, 2020.

[ds421] Raniyah Wazirali, Rami Ahmad, and Ashraf Abdel-Karim Abu-Ein. Sustaining accurate detection of phishing urls using sdn and feature selection approaches. *Computer Networks*, 201:108591, 2021.

[ds422] Guanglu Wei and Zhonghua Wang. Adoption and realization of deep learning in network traffic anomaly detection device design. *Soft Computing*, 25(2):1147–1158, 2021.

[ds423] Lei Wei and Carol Fung. Flowranger: A request prioritizing algorithm for controller dos attacks in software defined networks. In *2015 IEEE International Conference on Communications (ICC)*, pages 5254–5259. IEEE, 2015.

[ds424] Cameron S Whittle and Hong Liu. Effectiveness of entropy-based ddos prevention for software defined networks. In *2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–7. IEEE, 2021.

[ds425] Pengpeng Wu, Lin Yao, Chi Lin, Guowei Wu, and Mohammad S Obaidat. Fmd: A dos mitigation scheme based on flow migration in software-defined networking. *International Journal of Communication Systems*, 31(9):e3543, 2018.

[ds426] Xiaotong Wu, Meng Liu, Wanchun Dou, and Shui Yu. Ddos attacks on data plane of software-defined network: are they possible? *Security and communication networks*, 9(18):5444–5459, 2016.

[ds427] Peng Xiao, Zhiyang Li, Heng Qi, Wenyu Qu, and Haisheng Yu. An efficient ddos detection with bloom filter in sdn. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 1–6. IEEE, 2016.

[ds428] Rui Xiao, Hui Zhu, Chao Song, Ximeng Liu, Jian Dong, and Hui Li. Attacking network isolation in software-defined networks: new attacks and countermeasures. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–9. IEEE, 2018.

[ds429] Ya Xiao, Zhi-jie Fan, Amiya Nayak, and Cheng-xiang Tan. Discovery method for distributed denial-of-service attack behavior in sdns using a feature-pattern graph model. *Frontiers of Information Technology & Electronic Engineering*, 20(9):1195–1208, 2019.

[ds430] Zhao Xin-Hui, Wu Ze-Hui, Song Xiao-Bin, and Wang Qing-Xian. Secure analysis on entire software-defined network using coloring distribution model. *Concurrency and Computation: Practice and Experience*, page e5541, 2019.

[ds431] Jian-wen Xu, Kaoru Ota, Mian-xiong Dong, An-feng Liu, and Qiang Li. Siotfog: Byzantine-resilient iot fog networking. *Frontiers of information technology & electronic engineering*, 19(12):1546–1557, 2018.

[ds432] Jianfeng Xu, Liming Wang, and Zhen Xu. An enhanced saturation attack and its mitigation mechanism in software-defined networking. *Computer Networks*, 169:107092, 2020.

[ds433] Zhanyang Xu, Yanqi Zhang, Haoyuan Li, Weijing Yang, and Quan Qi. Dynamic resource provisioning for cyber-physical systems in cloud-fog-edge computing. *Journal of Cloud Computing*, 9(1):1–16, 2020.

[ds434] Cao Phan Xuan Qui, Dang Hong Quang, Phan The Duy, Do Thi Thu Hien, and Van-Hau Pham. Strengthening ids against evasion attacks with gan-based adversarial samples in sdn-enabled network. In *2021 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pages 1–6, 2021.

[ds435] Ming Xuanyuan, Visham Ramsurrun, and Amar Seeam. Detection and mitigation of ddos attacks using conditional entropy in software-defined networking. In *2019 11th International Conference on Advanced Computing (ICoAC)*, pages 66–71. IEEE, 2019.

[ds436] Aditya Yadav, Arpitha S Kori, Pooja Shettar, Mohammad M Moin, et al. A hybrid approach for detection of ddos attacks using entropy and machine learning in software defined networks. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2021.

[ds437] Sanjay Kumar Yadav, P Suguna, and R Leela Velusamy. Entropy based mitigation of distributed-denial-of-service (ddos) attack on control plane in software-defined-network (sdn). In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2019.

[ds438] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A security and trust framework for virtualized networks and software-defined networking. *Security and communication networks*, 9(16):3059–3069, 2016.

[ds439] Qussai Yaseen, Yaser Jararweh, Brajendra Panda, and Qutaibah Althebyan. An insider threat aware access control for cloud relational databases. *Cluster Computing*, 20:2669–2685, 2017.

[ds440] Abbas Yazdinejad, Reza M Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. *Computers and Security*, 88:101629, 2020.

[ds441] Changhoon Yoon, Seungsoo Lee, Heedo Kang, Taejune Park, Seungwon Shin, Vinod Yegneswaran, Phillip Porras, and Guofei Gu. Flow wars: Systemizing the attack surface and defenses in software-defined networks. *IEEE/ACM Transactions on Networking*, 25(6):3514–3530, 2017.

[ds442] Changhoon Yoon, Taejune Park, Seungsoo Lee, Heedo Kang, Seungwon Shin, and Zonghua Zhang. Enabling security functions with sdn: A feasibility study. *Computer Networks*, 85:19–35, 2015.

[ds443] Xiang You, Yaokai Feng, and Kouichi Sakurai. Packet in message based ddos attack detection in sdn network using openflow. In *2017 Fifth International Symposium on Computing and Networking (CANDAR)*, pages 522–528. IEEE, 2017.

[ds444] Mingli Yu, Tian Xie, Ting He, Patrick McDaniel, and Quinn K Burke. Flow table security in sdn: Adversarial reconnaissance and intelligent attacks. *IEEE/ACM Transactions on Networking*, 29(6):2793–2806, 2021.

[ds445] Shanshan Yu, Jicheng Zhang, Ju Liu, Xiaoqing Zhang, Yafeng Li, and Tianfeng Xu. A cooperative ddos attack detection scheme based on entropy and ensemble learning in sdn. *EURASIP Journal on Wireless Communications and Networking*, 2021(1):1–21, 2021.

[ds446] Zhipeng Yu, Hui Zhu, Rui Xiao, Chao Song, Jian Dong, and Hui Li. Detection and defense against network isolation attacks in software-defined networks. *Transactions on Emerging Telecommunications Technologies*, page e3895, 2020.

[ds447] Bin Yuan, Chen Lin, Deqing Zou, Laurence Tianruo Yang, and Hai Jin. Detecting malicious switches for a secure software-defined tactile internet. *ACM Trans. Internet Technol.*, 21(4), 2021.

[ds448] Meng Yue, Huaiyuan Wang, Liang Liu, and Zhijun Wu. Detecting dos attacks based on multi-features in sdn. *IEEE Access*, 8:104688–104700, 2020.

[ds449] Noe M. Yungaicela-Naula, Cesar Vargas-Rosales, Jesús Arturo Pérez-Díaz, and Mahdi Zareei. Towards security automation in software defined networks. *Computer Communications*, 183:64–82, 2022.

[ds450] Noe Marcelo Yungaicela-Naula, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. Sdn-based architecture for transport and application layer ddos attack detection by using machine and deep learning. *IEEE Access*, 9:108495–108512, 2021.

[ds451] Cinara Brenda Zerbini, Luiz Fernando Carvalho, Taufik Abrao, and Mario Lemes Proença Jr. Wavelet against random forest for anomaly mitigation in software-defined networking. *Applied Soft Computing*, 80:138–153, 2019.

[ds452] Bofeng Zhang, Li Han, and Shimin Sun. Dynamic random route mutation mechanism for moving target defense in sdn. In *2021 6th International Symposium on Computer and Information Processing Technology (ISCIPT)*, pages 536–541. IEEE, 2021.

[ds453] Menghao Zhang, Guanyu Li, Lei Xu, Jiasong Bai, Mingwei Xu, Guofei Gu, and Jianping Wu. Control plane reflection attacks and defenses in software-defined networks. *IEEE/ACM Transactions on Networking*, 29(2):623–636, 2020.

[ds454] Menghao Zhang, Guanyu Li, Lei Xu, Jiasong Bai, Mingwei Xu, Guofei Gu, and Jianping Wu. Control plane reflection attacks and defenses in software-defined networks. *IEEE/ACM Transactions on Networking*, 29(2):623–636, 2021.

[ds455] Peng Zhang, Hui Wu, Dan Zhang, and Qi Li. Verifying rule enforcement in software defined networks with rev. *IEEE/ACM Transactions on Networking*, 28(2):917–929, 2020.

[ds456] Dongcheng Zhao, Long Luo, Hongfang Yu, Victor Chang, Rajkumar Buyya, and Gang Sun. Security-sla-guaranteed service function chain deployment in cloud-fog computing networks. *Cluster Computing*, 24:2479–2494, 2021.

[ds457] Kaixin Zhao, Bo Lu, Hongyu Shi, Gang Ren, and Yang Zhang. A ddos attack detection and defense mechanism based on the self-organizing mapping in sdn. *Internet Technology Letters*, page e305.

[ds458] Rudong Zhao, Songjie Wei, and Milin Ren. Combating ddos attack with dynamic detection of anomalous hosts in software defined network. In *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, pages 37–42. IEEE, 2017.

[ds459] Xin Zhao, Lin Yao, and Guowei Wu. Esld: An efficient and secure link discovery scheme for software-defined networking. *International Journal of Communication Systems*, 31(10):e3552, 2018.

[ds460] Xinhui Zhao, Qingxian Wang, Zehui Wu, and Rui Guo. Method for overflow attack defense of sdn network flow table based on stochastic differential equation. *Wireless Personal Communications*, 117:3431–3447, 2021.

[ds461] Ma Zhao-hui, Zhao Gan-sen, Li Wei-wen, Mo Ze-feng, Wang Xin-ming, Chen Bing-chuan, and Lin Cheng-chuang. Research on ddos attack detection in software defined network. In *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, pages 1–6. IEEE, 2018.

[ds462] Wu Zhijun, Xu Qing, Wang Jingjie, Yue Meng, and Liu Liang. Low-rate ddos attack detection based on factorization machine in software defined network. *IEEE Access*, 8:17404–17418, 2020.

[ds463] Yuyang Zhou, Guang Cheng, and Shui Yu. An sdn-enabled proactive defense framework for ddos mitigation in iot networks. *IEEE Transactions on Information Forensics and Security*, 16:5366–5380, 2021.

[ds464] Liehuang Zhu, Xiangyun Tang, Meng Shen, Xiaojiang Du, and Mohsen Guizani. Privacy-preserving ddos attack detection using cross-domain traffic in software defined networks. *IEEE Journal on Selected Areas in Communications*, 36(3):628–643, 2018.

[ds465] Xian-wei Zhu and Chao-wen Chang. Packet access control mechanism based on cipher identification in software-defined network. In *Proceedings of the 2019 2nd International Conference on Information Management and Management Sciences*, pages 90–95. ACM, 2019.

[ds466] Zhibin Zuo, Chaowen Chang, Yong Zhang, Rongyu He, Xi Qin, and Kai Leung Yung. P4label: packet forwarding control mechanism based on p4 for software-defined networking. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–14, 2020.

ANDREA MELIS is currently an Adjunct Professor and a Postdoctoral Researcher with the Department of Computer Science and Engineering, University of Bologna. His research interest includes computer security related to innovative software architectures. In particular, his actual research activity aims to study, design and implement innovative solutions that allow to improve the safety, and operational robustness of connected production industrial networks and devices for cyber-security contexts.

AMIR AL SADI received the master's degree in computer science from Alma Mater Studiorum Universitã degli Studi di Bologna, Bologna, Italy, in 2021, where he is currently pursuing the Ph.D. degree in computer science and engineering. His research interests include software defined networking, programmable data plane, and network security.

DAVIDE BERARDI received the master's degree in computer science from Alma Mater Studiorum Universitã degli Studi di Bologna, Bologna, Italy, in 2016. He is currently a Postdoctoral Researcher in computer science and engineering with Alma Mater Studiorum, Universitã degli Studi di Bologna. His research interests include computer security, cyber security red teaming, and network virtualization.

FRANCO CALLEGATI (Senior Member, IEEE) is currently a Full Professor with the University of Bologna, Italy. His research interests include the teletraffic modeling and performance evaluation of telecommunication networks. He is also working on SDN/NFV networking, cybersecurity, and 5G. He has been active in EU-funded research projects, since FP4.

MARCO PRANDINI (Member, IEEE) is currently an Associate Professor with the Department of Computer Science and Engineering, University of Bologna. His research interests include public-key infrastructures and later moved to subjects related to the security of microservice-based architectures, software-defined networks, the IoT, and industrial control systems.

Open Access funding provided by 'Alma Mater Studiorum - Università di Bologna' within the CRUI CARE Agreement