Computers, Materials & Continua
DOI:10.32604/cmc.2021.016591
Article

Tech Science Press

Automated Controller Placement for Software-Defined Networks to Resist DDoS Attacks

Muhammad Reazul Haque[1], Saw Chin Tan[1], Zulfadzli Yusoff[2,*], Kashif Nisar[3,5,6], Lee Ching Kwang[2,7], Rizaludin Kaspin[4], Bhawani Shankar Chowdhry[5], Rajkumar Buyya[8], Satya Prasad Majumder[9], Manoj Gupta[10] and Shuaib Memon[11]

[1]Faculty of Computing & Informatics, Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Selangor, Malaysia
[2]Faculty of Engineering, Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Selangor, Malaysia
[3]Faculty of Computing and Informatics, University Malaysia Sabah, Jalan UMS, Kota Kinabalu Sabah, 88400, Malaysia
[4]Telekom Malaysia Research & Development, TM Innovation Centre, Cyberjaya, 63000, Selangor, Malaysia
[5]National Center of Robotics and Automation, Mehran University of Engineering & Technology, Jamshoro, Pakistan
[6]Department of Computer Science and Engineering, Hanyang University, Seoul, 04763, South Korea
[7]School of Electrical and Electronic Engineering, Nanyang Technological University, 639798, Singapore
[8]Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, Melbourne, VIC 3053, Australia
[9]Department of Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology (BUET), Dhaka, 1205, Bangladesh
[10]Department of Electronics and Communication Engineering, JECRC University, Vidhani, Jaipur, 303905, India
[11]Auckland Institute of Studies, Mt Albert, Auckland, New Zealand
[*]Corresponding Author: Zulfadzli Yusoff. Email: zulfadzli.yusoff@mmu.edu.my
Received: 05 January 2021; Accepted: 06 March 2021

Abstract: In software-defined networks (SDNs), controller placement is a critical factor in the design and planning for the future Internet of Things (IoT), telecommunication, and satellite communication systems. Existing research has concentrated largely on factors such as reliability, latency, controller capacity, propagation delay, and energy consumption. However, SDNs are vulnerable to distributed denial of service (DDoS) attacks that interfere with legitimate use of the network. The ever-increasing frequency of DDoS attacks has made it necessary to consider them in network design, especially in critical applications such as military, health care, and financial services networks requiring high availability. We propose a mathematical model for planning the deployment of SDN smart backup controllers (SBCs) to preserve service in the presence of DDoS attacks. Given a number of input parameters, our model has two distinct capabilities. First, it determines the optimal number of primary controllers to place at specific locations or nodes under normal operating conditions. Second, it recommends an optimal number of smart backup controllers for use with different levels of DDoS attacks. The goal of the model is to improve resistance to DDoS attacks while optimizing the overall cost based on the parameters. Our simulated results demonstrate that

the model is useful in planning for SDN reliability in the presence of DDoS attacks while managing the overall cost.

Keywords: SDN; automated controller placement; SBC; ILP; DDoS attack

1 Introduction

Software-defined networking (SDN) has gained prominence around the world because it is a programmable [1], cost-effective, agile, and centralized networking architecture compared to traditional systems that are more complicated and difficult to manage. The core of the SDN architecture is the primary controller that mediates between clients and resources to deliver services [2,3]. A generic depiction of the structure with connections between switches and primary controllers is shown in Fig. 1, with packets traveling from laptop A to laptop B. For example, a packet from laptop A will travel through OpenFlow switch 1 if the packet matches the predetermined flow table in switch 1 and, subsequently, through OpenFlow switches 2 and 3 until it reaches laptop B (route 4).

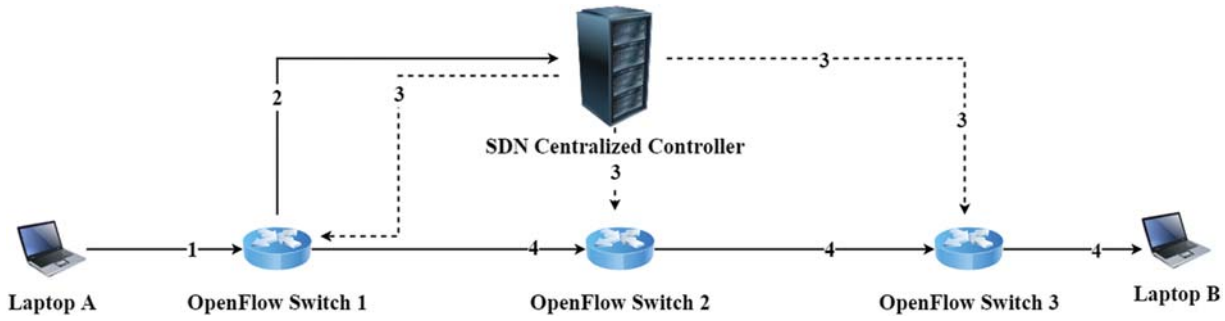

Figure 1: SDN controller workflow [4]

However, if the packet does not match the flow table at switch 1, the switch will then trigger the centralized primary controller (route 2) to update the flow table of that switch (route 3 in the figure). The same operational processes will be applied to the other OpenFlow switches 2 and 3.

The shortcoming of this structure is that the centralized primary controller is vulnerable to an attacker generating spoofed packets to infiltrate the primary controller. These hoax packets then spread to the other switches during flow table updates. This vicious cycle continues until the operation of the network comes to a halt, interrupting service as a result. Among all attacks, distributed denial of service (DDoS) attacks are among the most serious, generating huge amounts of artificial traffic to the SDN primary controller [5] and hampering its ability to provide services to legitimate clients. In OpenFlow [6], a switch requests new flow rules [7] from the primary controller if the switch experiences difficulty in forwarding data. The primary controller has the processing capability and responsibility for directing the flow of data packets. By sending massive numbers of spoofed packets not found in current flow tables, the DDoS attacker can overload the primary controller, which is unable to cope with the sudden influx of excessive fake packets, resulting in primary controller malfunction [8].

If the primary controller becomes the victim of a DDoS attack, all switches connected to that primary controller will malfunction and disrupt SDN services for legitimate users. Thus, DDoS

attacks are serious threats for SDNs. Hence, we propose using multiple backup primary controllers to provide uninterrupted services for primary controllers under DDoS attack.

Network availability is a key quality indicator of network planning design and planning [9]. Tab. 1 lists various availability requirements based on the priority of services demanded by clients. Military defense systems have the most stringent requirements among many network applications, requiring 99.9999% network availability, corresponding to a maximum of 31.5 s of downtime per year. Carrier-grade telephony, health, and banking systems are also demanding, requiring 99.999% availability, or a maximum outage time of 5 min and 15 s per year. Datacenters and high-end business systems require 99.99% uptime, allowing up to 52 min and 33 s of downtime per year. Currently, there is no single SDN primary controller that can provide adequate delivery security, reliability, and resiliency simultaneously [10–13].

Table 1: Network availability requirement per year

Class	Systems/Applications	Required uptime (%)	Maximum downtime
1	Military defense systems	99.9999	31.5 s
2	Carrier-grade telephony, health system and banking	99.999	5 min 15.36 s
3	Datacenters or high-end business system	99.99	52 min 33 s

SDN frameworks encounter many security threats, such as unauthorized primary controller access [14], corrupted or poisoned flow rules and forwarding policy discovery, primary controller-switch communication floods, and the DDoS-based switch flow table floods mentioned already [15]. The financial services industry was the third-most targeted industry by DDoS attacks in Q2 2019, as shown in Fig. 2 with gaming and high tech the best-known targets.

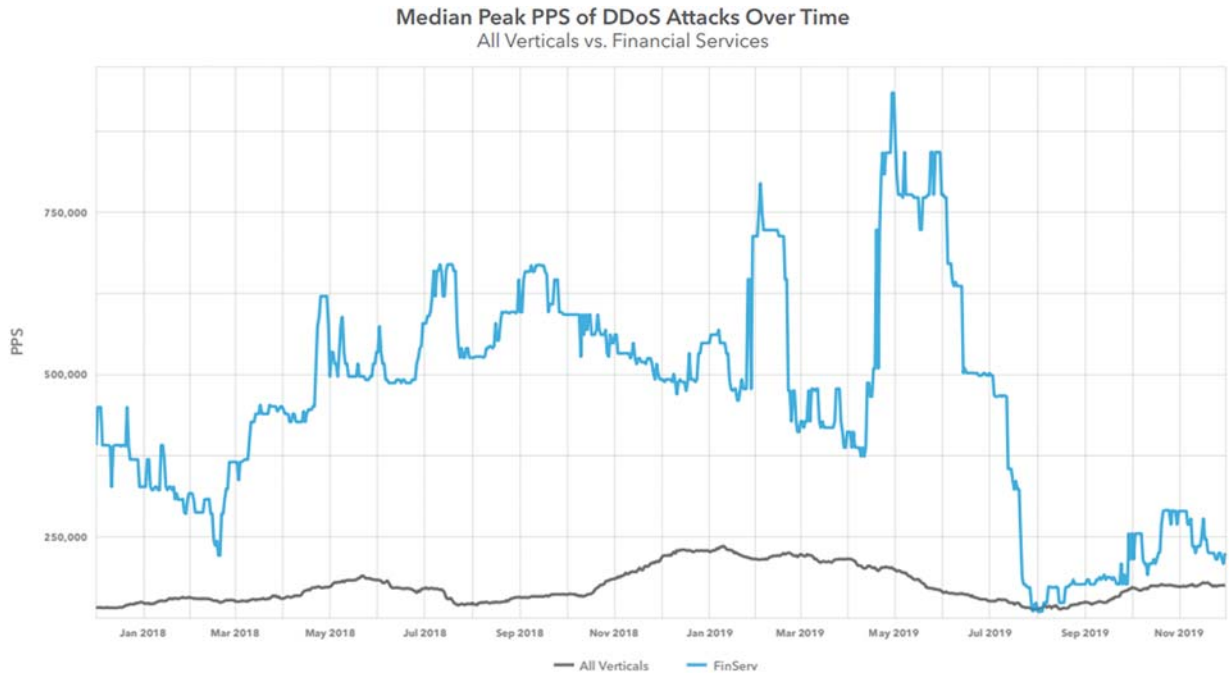

Figure 2: Peak DDoS PPS in financial services in May 2019 [16]

Worse, the frequency of DDoS attacks has been increasing dramatically as shown in Fig. 3 [17], with 58.3% of networks having been attacked more than once, 34.0% suffering 25 attacks, 11.2% encountering 6–10 attacks, and 13.1% experiencing more than 10 attacks in Q1 2017.

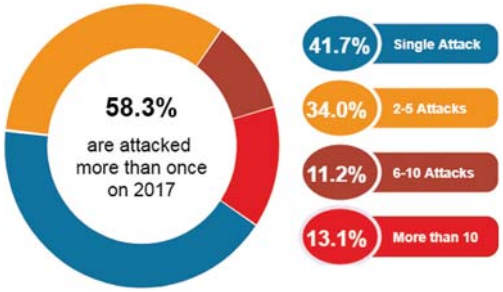

Figure 3: Frequency of DDoS attack in 2017 [18]

In Q1 2019, 40% of network experienced a single attack, 34% experienced 2–5 attacks, 7% experienced 6–9 attacks, and fully 19% experienced 10 or more attacks, as shown in Fig. 4.

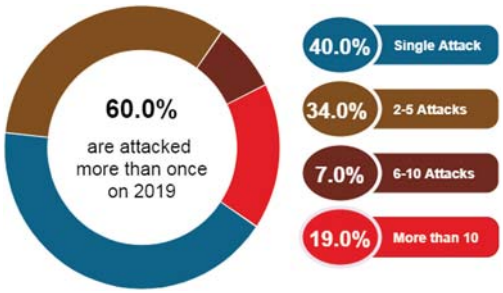

Figure 4: Persistence of DDoS attack on 2019 [19]

It is alarming that one company in the gaming industry experienced 558 attacks during the second quarter of 2017. By industry, 82% of gaming, 5% internet and telecom, 4% financial services, 42% software and technology, 2% media and entertainment, 1% retail and consumer goods, and 2% of education networks were repeatedly hit by DDoS attacks throughout the year 2017.

Multiple attacks have become more frequent as shown in Fig. 5. The average number of DDoS attacks per target was 30% in Q4 of 2016 and rose to 32% in Q2 of 2017. The duration of the attack needed to break the network has also been falling noticeably, thanks to sophisticated attack tools. In Q1 2017, the longest DDoS attack lasted around 204 h, a sharp decrease from the longest attack of 700 h in Q4 2016 and 483 hours in Q3 2016 [20]. Modern attack tools are causing primary controllers to fail in a shorter time.

Others have reported as shown in Fig. 6 that coercion in the form of threatened DDoS and ransom denial of service (RDoS) attacks have been made by an attacker claiming to attack for the sake of "Lazarus," compromising the victim's network if payment was not made within six days. Once the attack began, the attacker required an installment of 30 bitcoin (approx. $1500K) to stop it, with an extra 10 bitcoin ($500K) required for every day the payment remained unpaid [21].

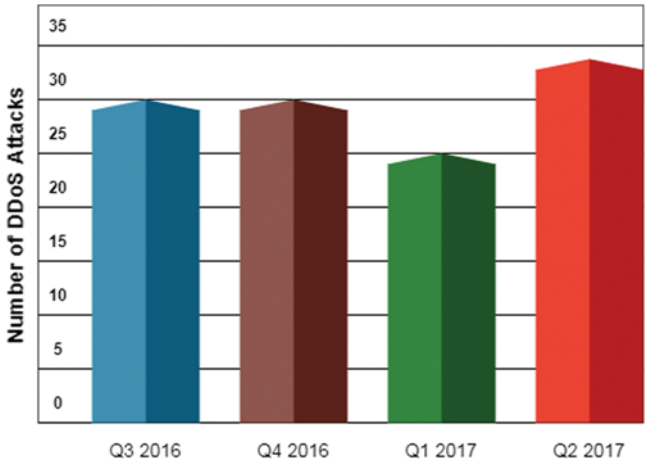

Figure 5: Average number of DDoS attacks per target, Q3 2016–Q2 2017

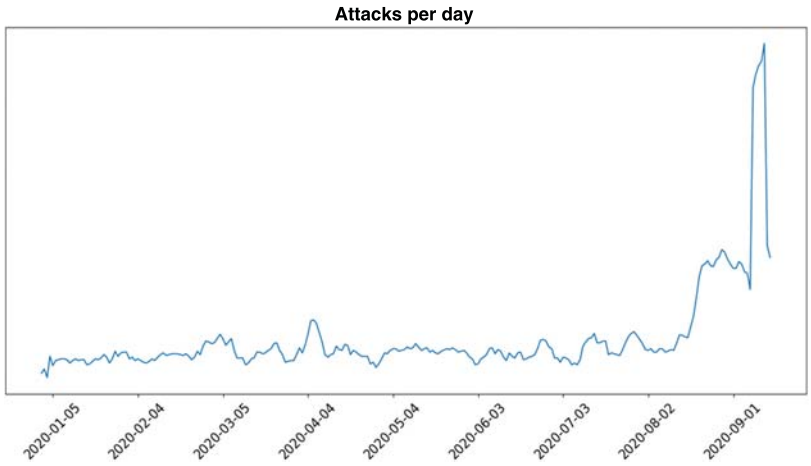

Figure 6: Number of DDoS attacks per day as observed in 2020

Thus, protecting SDN networks is turning out to be increasingly significant [22]. SDN provides rich network functions, the organization's utilization effectiveness is improved but SDNs have big security challenges simultaneously [23]: DDoS attacks, network interference, switch information spillage, and information confidentiality, along with traditional network attacks [24].

In this paper, we propose a new integer linear programming (ILP) mathematical model for planning the use of SDN smart backup controllers (SBCs) to resist DDoS attacks. The goal is to minimize the total cost of the SDN network during planning while determining the number and location of backup controllers to secure the network. We formulate the model using the occurrences and frequencies of DDoS attacks on the SDN primary controller.

We organize the rest of our paper as follows. In Section 2, we present related work. Section 3 presents our proposed smart backup controller placement mathematical model and formulation. Section 4 presents our experimental results and evaluation of the proposed model under various scenarios. We present our conclusions in Section 5.

2 Related Work

Before the existence of SDNs, several researchers had considered the goal of a networking system capable of fast, programmable data handling [25–31]. One proposal determined SDN primary controller placement using the k-median, and the k-center and their related optimization problem heuristic algorithms [32]. However, this proposal focused on the primary controller's latency, i.e., the primary controller's response time, and did not address primary controller placement with DDoS attacks. Others created a rule framework to adjust the links between the primary controller and switches based on the behavior of the primary controller placement problem [33]. Another proposal maximized the reliability of the SDN primary controllers using heuristic algorithms and brute force [34]. Others addressed the primary controller placement problem in reducing the worst latency of the control paths while satisfying the load constraints of the SDN primary controllers [35]. Without mentioning DDoS attacks, one author introduced an enhanced model for placing the SDN primary controller, switches, and links in the SDN [36]. Showing the vulnerability of SDN to DDoS attacks in cloud computing, researchers investigated the characteristics of DDoS attacks in cloud computing environments and gave a number of protective mechanisms for SDNs [37]. One proposal introduced a DDoS attack defense using a blocking system built upon the OpenFlow interface [38]. Another method used promptness, versatility, and accuracy to detect DDoS attacks [39]. For primary controller placement, one multiple-queue SDN primary controller scheduling algorithm used a time slice allocation strategy [40]. Others have used attack traffic, attack scale, and timelines to detect DDoS attacks in cloud services [41], but this method only detects attacks causing actual malfunctions and service disruptions.

pSMART is a lightweight and security-aware service function chain orchestration in network functions virtualization (NFV)/SDN situation. But it is incapable of supporting huge volumes of DDoS attack traffic [42]. Other proposed algorithms for precise and heuristic examinations which was created in the Matlab-based system for Pareto-based Optimal Controller placement [43]. However, it does not offer assistance during DDoS attacks. Other authors proposed a multiple objective ILP formulation to deduce primary controller placement, but this method does not consider security threats like DDoS attacks [44]. The Parameter Optimization Model (POM) for heuristic calculations has also been applied to controller placement problem (CPP) [45]. The heuristic algorithm adequately unravels the CPP by applying the advanced boundaries acquired in the POM, but the authors present no mechanism to protect the SDN primary controller and infrastructure. Another proposal used a hypothetical concept of smart controller placement for SDNs [46].

The use of SDNs is expanding, being used in applications such as voice over IP (VoIP) [47–49], fiber optic networks [50–52], worldwide interoperability for microwave access (WiMAX) networks [53–55], multiple input multiple output (MIMO) [56], Named Data Networking (NDN) [57–59] and cloud computing network [60], artificial intelligence (AI) and machine learning [ML] networks [61], and unmanned aerial vehicle (UAV) and autonomous electric vehicle (AEV) control through satellite networks [62]. The research into these topics has considered neither a smart backup controller nor the DDoS attack threat.

3 SDN Smart Backup Controller Placement and Problem Formulation

In this section, we introduce the problem of DDoS attack-aware controller placement using extra smart backup controllers to prevent service disruptions for legitimate users. Generally, primary controllers are connected to switches via a link, as shown in Fig. 7a.

We propose adding an extra controller, known as a smart backup controller, via a dynamic link [63], as illustrated in Fig. 7b. Our proposal activates the backup controller only when an original controller fails to function due to a DDoS attack. We build on earlier work on IP aliasing technique, which allocates multiple IP addresses to a single network interface, to create a unique dynamic switch to primary controller connection strategy [64,65]. By using this technique, the switch can statically connect to a single SDN primary controller at any given time while enabling reconnection to another primary controller dynamically and without reconfiguration [66].

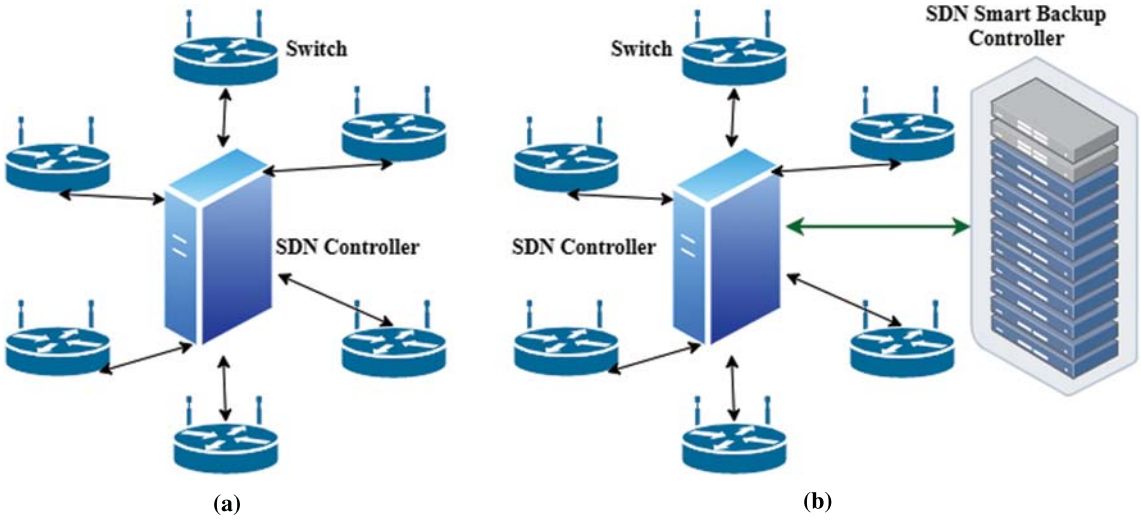

Figure 7: Existing and smart backup controller placement (a) Primary controller placement (b) Proposed smart backup controller placement

3.1 Parameters

Our method uses five important parameters:

- The number of primary controllers ($c \in C$) each of which may have a number of smart backup controllers ($b \in B$) based on the attack frequency $DDoS^{\eta}$.
- The maximum number of packet requests that primary controller μ^{c} or smart backup controller μ^{b} can handle per second;
- The distance $Range^{ab}$ and the bandwidth $\psi^{l}/Mbps$ availability for each link type connected between the primary controllers and the switches;
- The quantity of traffic ϕ^{s} to be sent from a switch to the primary controller; and
- The maximum latency for wireless $\nu^{(WirelessCom)}$ and wired communications $\nu^{(CopperWireCom)}$.

We also make use of several notations in formulating our model. These are described below.

3.2 Modulator

3.2.1 Sets of the Model

Symbol of sets of the model are listed in Tab. 2.

Table 2: Symbol of sets of the model

Sets	Descriptions
$\mathrm{SBC} = \{\mathrm{b1}, \mathrm{b2}, \mathrm{b3}, \ldots\}$,	The set of smart backup controllers ($b \in B$) that will be installed if a DDoS attack occurs on any primary controller.
λ^{b}	The number of ports of the smart backup controller ($b \in B$).
μ^{b}	The processing power of the smart backup controller of type ($b \in B$).
γ^{b}	The processing power of the smart backup controller ($b \in B$).
ρ^{b}	Different types of the available backup controller ($b \in B$) to install.
$\mathrm{C} = \{\mathrm{c1}, \mathrm{c2}, \mathrm{c3}, \ldots\}$,	The set of primary controllers ($c \in C$) that will be installed in SDN with the property, such as port, processing power, cost, and availability.
λ^{c}	The number of ports for each primary controller ($c \in C$).
μ^{c}	The processing power of each primary controller ($c \in C$).
γ^{c}	Cost of the primary controller ($c \in C$).
ρ^{c}	Different types of available primary controller ($c \in C$) to install.
$\delta = \{\mathrm{s1}, \mathrm{s2}, \mathrm{s3}, \ldots\}$,	The set of switches of type ($s \in \delta$) that will be connected to the primary controller.
ϕ^{s}	The number of available packets that does not have a match in the switch's ($s \in \delta$) flow table and that is sent to the installed primary controller to process.
$\zeta = \{\mathrm{l1}, \mathrm{l2}, \mathrm{l3}, \ldots\}$,	The set of link types ($l \in \zeta$) that connect primary controllers and switches.
ψ^{l}/Mbps	The bandwidth of the link type ($l \in \zeta$) in the byte.
ω^{l}/meter	The cost of the link of type ($l \in \zeta$) based on the bandwidth type. The cost is expressed in US$ per meter.
$\eta = \{\mathrm{n1}, \mathrm{n2}, \mathrm{n3}, \mathrm{n4}, \mathrm{n5}, \ldots\}$,	The set of the given nodes where primary controllers are placed.
$DDoS^{\eta} = \{1, 2, 3, \ldots\}$,	The set of possible attacks on the installed primary controller on a node ($n \in \eta$). The defined frequency of DDoS attacks ranges from 0 to 3 where 0 represents no attack, increasing to 3 for high frequency of attack. The model generates more smart backup controllers in the following scenarios: i) Network operations that require high availability such as military, health care, banking, and datacenters. ii) Those nodes that experience a higher-frequency of attack.

3.2.2 Constants

Several constants are used by our model. These are listed in Tab. 3.

3.2.3 Decision Variables of the SDN Model Under DDoS Attack

Several variables control the decisions made by our model. These are listed in Tab. 4.

Table 3: Constants used by the model

Constant	
$\theta^{\text{c or b}}$	Packet size in bytes to be processed by a primary controller type of ($c \in C$) or a smart backup controller type of ($b \in B$).
ξ	Speed of light to calculate the latency in wireless communication.
Range^{ab}	The range between two points a and b, expressing the distance between either two primary controllers or switches to the primary controller or backup controller to primary controller.
π	Function to convert the data packet size from Mbps or Gbps to the bytes.
$\kappa^{\text{c and b}}$	Processing time for the primary and smart backup controllers.
$\nu^{(\text{WirelessCom})}$	Maximum allowable latency using wireless communication.
$\nu^{(\text{CopperWireCom})}$	Maximum allowable latency using copper wire communication.

Table 4: Decision variables

Variables	Decision from variable matrix
T_{cn}	1, if a primary controller of type ($c \in C$) is installed at node ($n \in \eta$), else 0.
T_{bn}:	1, if a backup controller of type ($b \in B$) is installed at node ($n \in \eta$), else 0.
Z^{l}_{sn}:	1, if a link of type ($l \in \zeta$) is connected between switches type of ($s \in \delta$) and primary controller installed on the node ($n \in \eta$), else 0.
R^{l}_{nm}:	1, if a primary controller location ($n \in \eta$) is connected to a primary controller location ($m \in \eta$) with a link type ($l \in \zeta$), else 0.
R^{l}_{cb}	1, if a primary controller ($c \in C$) is connected to the smart backup controller ($b \in B$) with a link type ($l \in \zeta$), else 0.

3.3 Cost Functions

The objective of this mathematical model is to minimize the total cost of an SDN under DDoS attack. Cost depends on the number and types of primary controllers ($\text{Cost}^{c}(\text{T}^{c})$) installed in SDN; the smart backup controller placement with respect to the number and frequency of DDoS attacks ($\text{Cost}^{b}(\text{T}^{b})$); and the type of links between primary controllers ($\text{Cost}^{\zeta}(\text{R})$) between switches and primary controller ($\text{Cost}^{\zeta}(\text{Z})$) and $\text{Cost}^{\zeta}(R^{b})$ and between primary and smart backup controllers.

$$\text{Cost}^{c}(\text{T}^{c}) = \sum_{c \in \text{C}} \gamma^{c} \sum_{n \in \eta} \text{T}_{\text{cn}} \tag{1}$$

$$\text{Cost}^{b}(\text{T}^{b}) = \sum_{b \in B} \gamma^{b} \sum_{n \in \eta} \text{T}_{\text{bn}} \tag{2}$$

$$\text{Cost}^{\zeta}(\text{Z}) = \sum_{l \in \zeta} \omega^{l} \sum_{s \in \delta} \sum_{n \in \eta} \text{Range}^{sn} \cdot Z^{l}_{sn} \tag{3}$$

$$\text{Cost}^{\zeta}(\text{R}) = \sum_{l \in \zeta} \omega^{l} \sum_{m \in \eta} \sum_{\substack{n \in \eta \\ \text{m<n}}} \text{Range}^{\text{mn}} \cdot R^{l}_{nm} \tag{4}$$

$$\text{Cost}^{\zeta}(R^{b}) = \sum_{l \in \zeta} \omega^{l} \sum_{n \in \eta} \sum_{b \in B} \text{Range}^{nb} R^{l}_{cb}. \tag{5}$$

3.4 The SDN Model

The number of required smart backup controllers depends on the network availability requirements and the probabilities of the frequency of DDoS attacks on the SDN primary controller. We model our planning method as follows.

Objective Function :

Minimize

$$\mathrm{Cost}^{c}(\mathrm{T}^{c}) + \mathrm{Cost}^{b}(\mathrm{T}^{b}) + \mathrm{Cost}^{\zeta}(\mathrm{Z}) + \mathrm{Cost}^{\zeta}(\mathrm{R}) + \mathrm{Cost}^{\zeta}(R^{b})$$

Subject to

$$\sum_{c\in \mathrm{C}} \mathrm{T}_{cn} \sum_{b\in B} \mathrm{T}_{\mathrm{b}n} \geq \mathrm{DDoS}^{n} \quad (c \in \mathrm{C}, b \in B, n \in \eta) \tag{6}$$

This constraint places single or multiple smart backup controllers based on the frequency of DDoS attacks.

$$\sum_{l\in L} R^{l}_{cb} = \mathrm{T}_{\mathrm{b}n} \quad (n \in \eta, b \in B) \tag{7}$$

One link from the primary controller to the smart backup controller provides communication during DDoS attacks.

$$\frac{2\theta^{b}}{\psi^{l}} Z^{l}_{sn} + \sum_{b\in B} \frac{2\mathrm{Range}^{\mathrm{cb}}}{\xi} \mathrm{T}_{b\eta} + \varphi^{s}\mathrm{T}_{b\eta} \leq \nu \quad (n \in \eta, s \in \delta, l \in \zeta) \tag{8}$$

The latency of the smart backup controller depends on whether wireless or wired communication is used. Latency also varies for the distance between nodes in the SDN. The maximum latency of the smart backup controller must be smaller than the required latency. To calculate the latency, we multiply the one-way latency by 2 to obtain the round-trip distance and packet size of the data packet from a switch to the smart backup controller and the smart backup controller to a switch. The maximum latency of the smart backup controller must be smaller than the required latency.

$$\frac{2\theta^{c}}{\psi^{l}} Z^{l}_{\mathrm{sn}} + \sum_{c\in \mathrm{C}} \frac{2\mathrm{Range}^{\delta\eta}}{\xi} \mathrm{T}_{c\eta} + \varphi^{\delta}\mathrm{T}_{c\eta} \leq \nu \quad (n \in \eta, s \in \delta, l \in \zeta) \tag{9}$$

Same as constraint (8), this constraint (9) reflects primary controllers latency.

$$\sum_{b\in B} \mathrm{T}_{bn} \leq \rho^{b} \quad (n \in \eta) \tag{10}$$

The number of smart backup controller placements cannot be more than the number of smart backup controllers in inventory.

$$\sum_{c\in \mathrm{C}} \mathrm{T}_{cn} \leq \rho^{c} \quad (n \in \eta) \tag{11}$$

This constraint checks the availability of backup controllers before placing them.

$$\sum_{c\in \mathrm{C}} \mathrm{T}_{cn} \leq 1 \quad (n \in \eta) \tag{12}$$

Only one primary controller will be installed in each node to optimize the total SDN cost.

$$\sum_{l\in\zeta}\sum_{n\in\eta} Z_{sn}^{l} = 1 \quad (s \in \delta) \tag{13}$$

Each primary controller is connected to a switch with only one link.

$$\sum_{c\in \mathrm{C}} \mathrm{T}_{cm} + \sum_{c\in \mathrm{C}} \mathrm{T}_{cn} \leq \sum_{l\in\zeta} R_{nm}^{l} + 1 \quad (n \in \eta, m \in \eta, m > n) \tag{14}$$

A fully connected network or complete topology will be the topology for this SDN, depending on the decision of the SDN planner.

$$\sum_{m\in\eta}\sum_{l\in\zeta}\left(R_{nm}^{l} + R_{mn}^{l}\right) + \sum_{s\in\delta}\sum_{l\in\zeta} Z_{sn}^{l} \leq \sum_{c\in \mathrm{C}} \lambda^{c}\mathrm{T}_{cn} \quad (n \in \eta) \tag{15}$$

This constraint ensures that the number of switches and primary controllers does not exceed the available ports on the primary controller.

$$\sum_{m\in\eta}\sum_{l\in\zeta}\left(R_{\eta m}^{l} + R_{m\eta}^{l}\right) + \sum_{s\in\delta}\sum_{l\in\zeta} Z_{\mathrm{s}\eta}^{l} \leq \sum_{c\in \mathrm{B}} \lambda^{b}\mathrm{T}_{\mathrm{b}\eta} \quad (n \in \eta) \tag{16}$$

The following constraint ensures that the number of switches and backup controllers does not exceed the available ports of the smart backup controller

$$\sum_{s\in\delta} \varphi^{s}\theta^{c} \geq \sum_{c\in \mathrm{C}} \pi\psi^{l} Z_{\mathrm{s}\eta}^{l} \quad (n \in \eta) \tag{17}$$

The bandwidth of the link must be sufficient to carry the traffic between the switch and primary controller. This constraint converts the data packets into bytes.

$$\sum_{l\in\zeta}\sum_{s\in\delta} \varphi^{s} Z_{\mathrm{s}\eta}^{l} \leq \sum_{c\in \mathrm{C}} \mu^{c}\mathrm{T}_{c\eta} \quad (n \in \eta) \tag{18}$$

This constraint ensures that the processing power of the primary controller can support the data from the switches.

$$\sum_{l\in\zeta}\sum_{s\in\delta} \varphi^{s} Z_{\mathrm{s}\eta}^{l} \leq \sum_{c\in \mathrm{B}} \mu^{b}\mathrm{T}_{\mathrm{b}\eta} \quad (n \in \eta) \tag{19}$$

This constraint ensures that the processing power of the smart backup controller can support the data from the switches.

The values used in the computation are listed in Tabs. 5–8. The costs of the primary controllers, smart backup controllers, and bandwidth are hypothetical averages of current prices due to variations across providers.

Table 5: Primary controller parameters

Primary controller type	λ^c	μ^c	γ^c	ρ^c
C1	8	2500	\$1000	20
C2	32	4000	\$2000	15
C3	64	8000	\$4500	10
C4	16	5500	\$5000	28
C5	64	6000	\$7000	19
C6	128	13000	\$9500	12
C7	16	5500	\$5000	28
C8	64	6000	\$7000	19
C9	128	13000	\$9500	12

Table 6: Smart backup controller parameters

Smart backup controller type	λ^b	μ^b	γ^b	ρ^b
b1	8	3500	\$1200	20
b2	64	6000	\$2300	25
b3	128	9000	\$5500	30
b4	16	4500	\$2200	20
b5	64	6000	\$2500	25
b6	256	16000	\$9500	40
b7	256	16000	\$9500	30

Table 7: Link parameters

Link type	ψ^l/Mbps	ω^l/meter
l1	10000000	\$0.25
l2	200000000	\$0.63
l3	10000000000	\$29

Table 8: Switches with data size and constant with data

Switch type	ϕ^s	Constant type	Data
S1	100	$\theta^{c \text{ or } b}$	500 bytes
S2	800	ξ	299792458 m/s
S3	700	$Range^{\delta\eta}$	100 m
S4	6000	$Range^{m\eta}$	100 m
S5	5000	$Range^{cb}$	1 m
S6	700	π	1/8
S7	6000	$\kappa^{c \text{ and } b}$	0.000001 ms
S8	900	$\nu^{(WirelessCom)}$	10,000 ms
S9	9000	$\nu^{(CopperWireCom)}$	300000000000 ms

4 Experimental Result and Evaluation

We implemented our proposed model using AMPL (A Mathematical Programming Language) [67] and IBM ILOG CPLEX [68]. Our test hardware was a system with an Intel Core i7–6700 CPU at 3.40 GHz, 8 GB of RAM, and virtual memory 128 GB machine, we created 128 GB storage of hard disk as artificial RAM. We evaluated our proposed model in several different scenarios for both of its major functions: Planning primary controller and node placement in view of anticipated traffic and determining smart backup controller placement to resist various levels of DDoS attacks.

4.1 SDN Primary Controller Placement Without DDoS Attack

Tab. 9 presents a summary of the node and primary controller placement results of our model for five representative scenarios.

Table 9: IBM ILOG CPLEX solutions for five different problems without DDoS attack

S#	δ	ζ	G η/η	C	Packets per second	Cost (US$)	Processing time (s)
1	5	6	9/2	2	12,600	9350	0.125
2	5	11	30/4	4	27,000	18850	7.8125
3	12	27	12/6	6	6,600	9300	23.1562
4	5	6	100/2	2	12,600	9350	893.547
5	9	12	7/4	4	29,200	24050	0.34375

In Scenario 1, the input node (Gη) was 9 (9 primary controllers deployed at 9 nodes). Our model proposed 2 nodes (η) with 2 primary controllers (C), 5 switches (δ), and 6 links (ζ). This result saved 7 primary controllers and 7 nodes in total. The total available data packets per second were 12,600, within the abilities of 2 primary controllers.

In Scenario 2, the input node (Gη) value was 30 (30 primary controllers deployed at 30 nodes). Our model proposed 2 nodes (η) with 2 primary controllers (C), 5 switches (δ), and 11 links (ζ). This result saved 29 primary controllers and 28 nodes in total. The total available data packets per second were 27,000. CPLEX took 7.8 s to reach this result.

In Scenario 3, the input node (Gη) value was 12 (12 primary controllers deployed at 12 nodes). Our model proposed 6 nodes (η) with 6 primary controllers (C), 12 switches (δ), and 27 links (ζ). This result saved 6 primary controllers and 6 nodes in total. The total available data packets per second were 6,600.

In Scenario 4, the input node (Gη) value was 100 (100 primary controllers deployed at 100 nodes). Our model proposed 2 nodes (η) with 2 primary controllers (C), 5 switches (δ), and 6 links (ζ). This result saved 98 primary controllers and 98 nodes in total. The total available data packets per second were 12,600. However, finding this result required 893.5 s due to the large number of inputs.

Finally, in Scenario 5, the input node (Gη) value was 7 (7 primary controllers deployed at 7 nodes). Our model proposed 4 nodes (η) with 4 primary controllers (C), 9 switches (δ), and 12 links (ζ). This result saved 3 primary controllers and 3 nodes in total. The total available data packets per second were 29,200. Finding this result required 0.34375 s.

These results show that the total cost of an SDN depends on the capacity of each primary controller, expected volume of data packets, and the bandwidth of the links.

4.2 SDN Smart Backup Controller Placement Under Different Frequencies of DDoS Attacks

We further evaluated our proposed model in placing backup controllers to preserve services on various levels of DDoS attacks. Results for this test are given in Tab. 10 for 9 representative scenarios.

Table 10: Smart Backup controller placement with single and multiple DDoS attacks on the primary controller

Scenario#	Frequency of DDoS attack	DDoS attack on primary controller (DAC)	Smart backup controller (SBC) placement	Cost (US$)
1	No Attack (0)	0	0	23,950
2	Low Attack (1)	1	1	25,150
3		2	2	26,350
4	Medium Attack (2)	1	2	27,650
5		2	4	31,350
6		3	6	35,050
7	High Attack (3)	1	3	33,150
8		2	6	42,350
9		3	9	51,550
	The total cost includes primary controller, SBC, bandwidth, and link costs.			

In Scenario 1, our proposed model assigned no backup controllers because there was no attack on the primary controller, with a total cost of $23,950. This cost contains only the SDN setup cost.

In Scenario 2, only one smart backup controller was installed because only one DDoS attack was planned. The total cost was $25,150, representing the SDN setup with a single backup controller.

Scenario 3 resulted in placing two backup controllers after detecting two planned DDoS attacks on two different primary controllers. The total cost increased to $26,350.

Scenario 4 included detection of medium (double) frequency of DDoS attacks on one primary controller. The medium attack represented two DDoS attacks on one primary controller. Our model recommended two backup controllers for uninterrupted SDN services.

In Scenario 5, our system considered two detected medium frequency DDoS attacks and recommended four different types of backup controllers, at a total cost of $31,350.

In Scenario 6, our method proposed six SBCs after detecting three medium frequencies of DDoS attacks with a total cost of $31,350.

Scenario 7 introduced a high level of DDoS attacks, representing a triple DDoS attack on a single SDN primary controller. Our model recommended three backup controllers, for a total cost of $33,150.

In Scenario 8, our method recommended 6 SBCs after considering two high frequency of DDoS attacks.

Finally, in Scenario 9, our method considered three high-frequency DDoS attacks on three different SDN primary controllers. It recommended 9 SBCs, for a total cost of $51,550.

The results of these scenarios show that our model is capable of securing SDNs against DDoS attacks by using additional backup controllers in conjunction with the existing SDN controller.

The required cost to secure these networks is plotted in Fig. 8. The cost ranged from below $30,000 for no attack to around $50,000 for protecting against triple attacks. Clearly, less protection has a lower cost, and more protection has a higher cost.

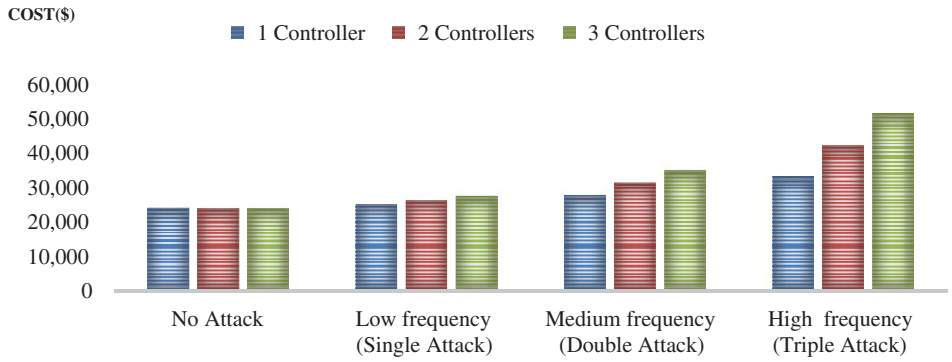

Figure 8: Cost for securing SDNs for different frequencies of DDoS attacks

5 Conclusions and Future Work

The purpose of our work has been to propose a model for securing a software-defined network against varying levels of DDoS attacks on its primary controller through the use of additional smart backup controllers (SBCs). We have defined our method to minimize the overall cost while providing the needed protection. Our simulation results demonstrate that our proposed model is able to counter DDoS attacks by careful placement of backup controllers and to preserve uninterrupted service for legitimate users. Our proposed model is robust and useful for planning SDNs, especially for critical applications such as military, health care, satellite, and financial services networks that require high network availability. In future work, we plan to extend our proposed model to the deployment of Next-Generation SDN (NG-SDN) and CORD hardware architecture environments. We also plan to implement our proposed model with additional parameters to support machine learning capabilities, Internet of Things (IoT) devices, UAV & EV connectivity through satellite links, cloud computing, and protect data losses.

Acknowledgement: The authors would like to thank the editors of CMC and anonymous reviewers for their time and for reviewing this manuscript and Professor Dr. Yong-Jin Park (IEEE Life member and former Director IEEE Region 10) for his valuable comments and suggestions on improving the paper. Finally, special thanks to the LetPub editors for their great proofreading support.

Funding Statement: This research work was funded by TMR&D Sdn Bhd under project code RDTC160902.

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

References

[1] C. Ren, S. Bai, Y. Wang and Y. Li, "Achieving near-optimal traffic engineering using a distributed algorithm in hybrid SDN," *IEEE Access*, vol. 8, pp. 29111–29124, 2020.

[2] K. Nisar, E. R. Jimson, M. H. A. Hijazi, I. Welch, R. Hassan *et al.,* "A survey on the architecture, application, and security of software defined networking," *Internet of Things*, vol. 12, no. 5, pp. 1–27, 2020.

[3] E. R. Jimson, K. Nisar and M. H. A. Hijazi, "The state of the art of software defined networking (SDN): Network management solution in current network architecture using the SDN," *International Journal of Information Communication Technologies and Human Development*, vol. 10, no. 4, pp. 44–60, 2018.

[4] K. Sood and Y. Xiang, "The controller placement problem or the controller selection problem?," *Journal of Communications and Information Networks*, vol. 2, no. 3, pp. 1–9, 2017.

[5] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusam *et al.,* "An evolutionary SVM model for DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020.

[6] X. Shi, Y. Li, H. Xie, T. Yang, L. Zhang *et al.,* "An openflow-based load balancing strategy in SDN," *Computers, Materials & Continua*, vol. 62, no. 1, pp. 385–398, 2020.

[7] M. R. Haque, S. C. Tan, C. K. Lee, Z. Yusoff, S. Ali *et al.,* "Analysis of DDoS attack-aware software-defined networking controller placement in Malaysia," in *Recent Trends in Computer Applications*, Cham, Switzerland: Springer International Publishing AG, Springer Nature, pp. 175–188, 2018.

[8] M. Ruaro, L. L. Caimi and F. G. Moraes, "A systemic and secure SDN framework for noc-based many-cores," *IEEE Access*, vol. 8, pp. 105997–106008, 2020.

[9] B. Mitchell, "Concepts for networks and systems," in *Lifewire*, New York, USA: Dotdash Publishing Family, 2020. [Online]. Available: https://www.lifewire.com/availability-concepts-for-networks-systems-817820.

[10] A. Shirmarz and A. Ghaffari, "Performance issues and solutions in SDN-based datacenter: A survey," *Journal of Supercomputing*, vol. 74, no. 10, pp. 7545–7593, 2020.

[11] M. Karakus and A. Durresi, "Quality of service (QoS) in software defined networking (SDN): A survey," *Journal of Network and Computer Applications*, vol. 80, no. 2015, pp. 200–218, 2017.

[12] J. Shuja, R. W. Ahmad, A. Gani, A. I. A. Ahmed, K. Nisar *et al.,* "Greening emerging it technologies: Techniques and practices," *Journal of Internet Services and Applications*, vol. 8, no. 9, pp. 1–11, 2017.

[13] I. A. Lawal, A. M. Said, K. Nisar and A. A. Mu'azu, "A distributed QoS-oriented model to improve network performance for fixed WiMAX," *International Journal on Recent Trends in Engineering and Technology*, vol. 10, no. 1, pp. 186–202, 2014.

[14] K. Nisar, E. R. Jimson, M. H. A. Hijazi, A. A. A. Ibrahim, Y. J. Park *et al.,* "A new bandwidth management model using software-defined networking security threats," in *IEEE 13th Int. Conf. on Application of Information and Communication Technologies*, Baku, Azerbaijan, pp. 1–3, 2019.

[15] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[16] J. Leggio and M. McKeay, "Financial services—Hostile takeover attempts," *Akamai*, vol. 6, no. 1, pp. 13–14, 2020. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf.

[17] I. Zeifman, "Q1 2017 Global DDoS threat landscape report, incapsula, blog, bots & DDoS, security," *Incapsula*, 2017. [Online]. Available: https://www.incapsula.com/blog/q1-2017-global-ddos-threat-landscape-report.html.

[18] M. McKeay, "Q2 2017 State of the internet security report," *Akama*, 2017. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf.

[19] J. G. McKeever and J. Azaria, "Major global ransom denial of service campaign continues rising trend in global DDoS attacks," *Imperva Research Labs*, 2020. [Online]. Available: https://www.imperva.com/blog/major-global-ransom-denial-of-service-campaign-continues-rising-trend-in-global-ddos-attacks/.

[20] Imperva, "Global DDoS Threat Landscape," *Incapsula*, 2017. [Online]. Available: https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html.

[21] G. McKeever and J. Azaria, "DDoS report 2019: Global DDoS threat landscape," *Imperva Research Labs*, 2020. [Online]. Available: https://www.imperva.com/resources/resource-library/reports/global-ddos-threat-landscape.

[22] W. Zhijun, X. Qing, W. Jingjie, Y. Meng and L. Liang, "Low-rate DDoS attack detection based on factorization machine in software defined network," *IEEE Access*, vol. 8, pp. 17404–17418, 2020.

[23] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, C. K. Lee *et al.,* "A novel DDoS attack-aware smart backup controller placement in SDN design," *Annals of Emerging Technologies in Computing*, vol. 4, no. 5, pp. 75–92, 2020.

[24] S. Shin, V. Yegneswaran, P. Porras and G. Gu, "Avant-guard: Scalable and vigilant switch flow management in software-defined networks," in *CCS '13: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications*, NY, USA, pp. 413–424, 2013.

[25] R. D. Lallo, F. Griscioli, G. Lospoto, H. Mostafaei, M. Pizzonia *et al.,* "Leveraging SDN to monitor critical infrastructure networks in a smarter way," in *IFIP/IEEE Symp. on Integrated Network and Service Management*, Lisbon, pp. 608–611, 2017.

[26] M. B. Anwer, M. Motiwala, M. Tariq and N. Feamster, "Switchblade: A platform for rapid deployment of network protocols on programmable hardware," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 183–194, 2010.

[27] H. I. Kobo, A. M. Abu-Mahfouz and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.

[28] M. R. Haque, S. C. Tan, Z. Yusoff, C. K. Lee, S. Ali *et al.,* "Motivation of DDoS attack-aware in software defined networking controller placement," in *Int. Conf. on Computer and Applications*, Dubai, pp. 36–42, 2017.

[29] J. Yang, Z. Yao, B. Yang, X. Tan, Z. Wang *et al.,* "Software-defined multimedia streaming system aided by variable-length interval in-network caching," *IEEE Transactions on Multimedia*, vol. 21, no. 2, pp. 494–509, 2019.

[30] S. Han, K. Jang, K. Park and S. Moon, "Packetshader: A GPU-accelerated software router," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 1–12, 2010.

[31] K. Nisar, E. R. Jimson, M. Hijazi and K. S. Memom, "Memon A survey: Architecture, security threats and application of SDN," *Journal of Industrial Electronics Technology and Application*, vol. 2, no. 1, pp. 64–69, 2019. [Online]. Available: http://jieta.org/v2n101/.

[32] B. Heller, R. Sherwood and N. McKeown, "The controller placement problem," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 473–478, 2012.

[33] M. F. Bari, A. R. Roy, S. R. Chowdhury, Q. Zhang, M. F. Zha *et al.,* "Dynamic controller provisioning in software defined networks," in *Proc. of the 9th Int. Conf. on Network and Service Management*, Zurich, Switzerland, pp. 18–25, 2013.

[34] Y. N. Hu, W. D. Wang, X. Y. Gong, X. R. Que and S. D. Cheng, "On the placement of controllers in software-defined networks," *Journal of China Universities of Posts and Telecommunications*, vol. 19, no. 5, pp. 92–97, 2012.

[35] G. Yao, J. Bi, Y. Li and L. Guo, "On the capacitated controller placement problem in software defined networks," *IEEE Communications Letters*, vol. 18, no. 8, pp. 1339–1342, 2014.

[36] A. Sallahi and M. St-Hilaire, "Expansion model for the controller placement problem in software defined networks," *IEEE Communications Letters*, vol. 21, no. 2, pp. 274–277, 2017.

[37] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 52–59, 2015.
[38] S. Lim, J. Ha, H. Kim, Y. Kim and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," in *2014 Sixth Int. Conf. on Ubiquitous and Future Networks*, Shanghai, pp. 63–68, 2014.
[39] T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh *et al.,* "Defending against new-flow attack in SDN-based internet of things," *IEEE Access*, vol. 5, pp. 3431–3443, 2017.
[40] Q. Yan, Q. Gong and F. R. Yu, "Effective software-defined networking controller scheduling method to mitigate DDoS attacks," *Electronics Letters*, vol. 53, no. 7, pp. 469–471, 2017.
[41] J. Zhang, P. Liu, J. He and Y. Zhang, "A hadoop based analysis and detection model for IP spoofing typed DDoS attack," in *IEEE Trustcom/BigDataSE/ISPA*, Tianjin, pp. 1976–1983, 2016.
[42] K. D. Joshi and K. Kataoka, "Psmart: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN," *Computer Networks*, vol. 178, no. 2, pp. 107295, 2020.
[43] S. Lange, S. Gebert, T. Zinner, P. Tran-Gia, D. Hock *et al.,* "Heuristic approaches to the controller placement problem in large scale SDN networks," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 4–17, 2015.
[44] T. Das and M. Gurusamy, "Controller placement for resilient network state synchronization in multi-controller SDN," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1299–1303, 2020.
[45] Y. Li, S. Guan, C. Zhang and W. Sun, "Parameter optimization model of heuristic algorithms for controller placement problem in large scale SDN," *IEEE Access*, vol. 8, pp. 151668–151680, 2020.
[46] M. R. Haque, S. C. Tan, Z. Yusoff, C. K. Lee and R. Kaspin, "DDoS Attack monitoring using smart controller placement in software defined networking architecture," In: R. Alfred, Y. Lim, A. Ibrahim, P. Anthony (Eds). *Computational Science and Technology. Lecture Notes in Electrical Engineering*. vol. 481, Singapore: Springer, 2019. [Online]. Available: https://doi.org/10.1007/978-981-13-2622-6_2046.
[47] K. Nisar, A. Amphawan, S. Hassan and N. I. Sarkar, "A comprehensive survey on scheduler for VoIP over WLANS," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 933–948, 2013.
[48] F. Sattar, M. Hussain and K. Nisar, "A secure architecture for open source VoIP solutions," in *Int. Conf. on Information and Communication Technologies*, Karachi, pp. 1–6, 2011.
[49] K. Nisar, A. M. Said and H. Hasbullah, "Enhanced performance of packet transmission using system model over VoIP network," in *IEEE Int. Symp. on Information Technology*, Kuala Lumpur, Malaysia, pp. 1005–1008, 2010.
[50] S. Chaudhary, A. Amphawan and K. Nisar, "Realization of free space optics with OFDM under atmospheric turbulence," *Optik*, vol. 125, no. 18, pp. 5196–5198, 2014.
[51] A. Amphawan, V. Mishra, K. Nisar and B. Nedniyom, "Real-time holographic backlighting positioning sensor for enhanced power coupling efficiency into selective launches in multimode fiber," *Journal of Modern Optics, OX14 4RN United Kingdom*, vol. 59, no. 20, pp. 1745–1752, 2012.
[52] R. Singh and G. Soni, "Realization of OFDM based free space optics," in *Int. Conf. on Green Computing and Internet of Things*, Noida, pp. 32–35, 2015.
[53] Z. Yan, G. Geng, H. Nakazato, Y. Park, K. Nisar *et al.,* "On-demand DTN communications in heterogeneous access networks based on NDN," in *2017 IEEE 85th Vehicular Technology Conf.*, Sydney, NSW, pp. 1–2, 2017.
[54] L. X. Wee, Z. Yan, Y. J. Park, Y. Leau, K. Nisar *et al.,* "Rom-p: Route optimization management of producer mobility in information-centric networking," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. vol. 267. Cham: Springer, pp. 81–91, 2019.
[55] I. A. Lawal, A. M. Said, K. Nisar, P. A. Shah and A. R. A. Mu'azu, "Throughput performance improvement for VoIP applications in fixed WiMAX network using client-server model," *Journal of Science International*, vol. 26, no. 3, pp. 999–1002, 2014. [Online]. Available: http://www.sci-int.com/pdf/636639048130555148.%20Lawal–.pdf.
[56] T. H. Dahawi, Z. Yusoff, M. S. Salleh and J. M. Senior, "Low-cost MIMO-RoF-PON architecture for next-generation integrated wired and wireless access networks," *Journal of Optical Communications and Networking*, vol. 13, no. 3, pp. 41–52, 2021.

[57] A. A. A. Ibrahim and K. Nisar, "Future internet and named data networking hourglass, packet and node architecture," *Journal of Industrial Information Technology and Application*, vol. 2, no. 3, pp. 115–123, 2018.

[58] S. Zhang, Z. Yan, Y. Park, H. Nakazatod, W. Kameyama *et al.,* "Efficient producer mobility support in named data networking," in *The Institute of Electronics, Information and Communication Engineers, The IEICE Transactions*, Tokyo, Japan, vol. E100-B, pp. 1856–1864, 2017.

[59] S. Harada, Z. Yan, Y. Park, K. Nisar and A. A. A. Ibrahim, "Data aggregation in named data networking," in *IEEE Region 10 Conf.*, Penang, Malaysia, pp. 1839–1842, 2017.

[60] Y. Zhang, X. Lan, J. Ren and L. Cai, "Efficient computing resource sharing for mobile edge-cloud computing networks," *IEEE/ACM Transactions on Networking*, vol. 28, no. 3, pp. 1227–1240, 2020.

[61] S. Shahzadi, F. Ahmad, A. Basharat, M. Alruwaili, S. Alanazi *et al.,* "Machine learning empowered security management and quality of service provision in SDN-NFV environment," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2723–2749, 2021.

[62] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, C. K. Lee *et al.,* "SDN architecture for UAVs and EVs using satellite: A hypothetical model and new challenges for future," in *CCNC 2021 WKSHPS TCB6GN*, USA, 2021.

[63] Y. E. Oktian, S. Lee, H. Lee and J. Lam, "Distributed SDN controller system: A survey on design choice," *Computer Networks*, vol. 121, no. 4, pp. 100–111, 2017.

[64] V. Yazici, M. O. Sunay and A. O. Ercan, "Controlling a software-defined network via distributed controllers," in *arXiv*, New York, USA: Cornell University, pp. 16–20, 2014. [Online]. Available: https://arxiv.org/abs/1401.7651.

[65] A. E. Kamel and H. Youssef, "Improving switch-to-controller assignment with load balancing in multi-controller software defined wan (SD-WAN)," *Journal of Network and Systems Management*, vol. 28, no. 3, pp. 553–575, 2020.

[66] S. Manzoor, Z. Chen, Y. Gao, X. Hei and W. Cheng, "Towards QoS-aware load balancing for high density software defined Wi-Fi networks," *IEEE Access*, vol. 8, pp. 117623–117638, 2020.

[67] R. Fourer, D. Gay and B. Kernighan, "A Mathematical Programming Language, (AMPL)," 2020. [Online]. Available: https://ampl.com.

[68] IBM ILOG CPLEX, "Optimization Studio," 2020. [Online]. Available: https://www.ibm.com/products/ilog-cplex-optimization-studio.