Annals of Emerging Technologies in Computing (AETiC)
Vol. 4, No. 5, 2020

Research Article

A Novel DDoS Attack-aware Smart Backup Controller Placement in SDN Design

Muhammad Reazul Haque[1], Saw Chin Tan[1], Zulfadzli Yusoff[1], Kashif Nisar[2,3,5,*], Ching Kwang Lee[1], Rizaludin Kaspin[4], BS Chowdhry[5], Sameer Ali[6] and Shuaib Memon[7]

[1]Multimedia University, 63100 Cyberjaya, Malaysia
reazulh@gmail.com; sctan1@mmu.edu.my; zulfadzli.yusoff@mmu.edu.my; cklee@mmu.edu.my
[2]University Malaysia Sabah, Jalan UMS, 88400, Kota Kinabalu, Sabah, Malaysia
kashif@ums.edu.my
[3]Hanyang University, Seoul, South Korea
kashifnisar@ieee.org
[4]TM Innovation Centre, Telekom Malaysia, 63100, Cyberjaya, Malaysia
rizaludin@tmrnd.com.my
[5]Mehran University of Engineering & Technology, Jamshoro, Pakistan
bhawani.chowdhry@faculty.muet.edu.pk
[6]Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Karachi, Pakistan
sameer.ali@szabist.edu.pk
[7]Auckland Institute of Studies, Mt Albert, Auckland, New Zealand
shuaibm@ais.ac.nz
*Correspondence: kashif@ums.edu.my

Received: 8th November 2020; Accepted: 17th December 2020; Published: 20th December 2020

Abstract: Security issues like Distributed Denial of Service (DDoS) attacks are becoming the main threat for Software-Defined Networking (SDN). Controller placement is a fundamental factor in the design and planning of SDN infrastructure. The controller could be seen as a single dot of failure for the whole SDN and it's the alluring point for DDoS attack. Single controller placement implies a single point of SDN control. So, there is a very high chance to fail the entire network topology as the controller associated with all switches. As a result, legitimate clients won't have the capacity to use SDN services. This is the reason why the controller is the suitable center dot of attack for the aggressor. To protect SDN from this type of single purpose of failure, it is essential to place multiple smart backup controllers to guarantee the SDN operation. In this paper, we propose a novel Integer Linear Programming (ILP) model to optimize the security issue by placing powerful smart backup controller. Result obtained from the simulation shows that our proposed novel ILP model can suggest single or multiple smart backup controller placement to support several ordinary victim controllers which has the capacity to save the cost of multiple ordinary controllers by sharing link, maximum new flows per second of controller and port, etc.

Keywords: ***Smart Backup Controller Placement; SDN Design; DDoS Attack-Aware; Cloud Network Security***

1. Introduction

Software-Defined Networking (SDN) innovation is a novel way to deal with cloud computing, data center, Internet of Things (IoT) and telecommunication network to enhance network performance and observing network management centrally. SDN recommends unifying network

Muhammad Reazul Haque, Saw Chin Tan, Zulfadzli Yusoff, Kashif Nisar, Ching Kwang Lee, Rizaludin Kaspin, BS Chowdhry, Sameer Ali and Shuaib Memon, "A Novel DDoS Attack-aware Smart Backup Controller Placement in SDN Design", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 75-92, Vol. 4, No. 5, 20th December 2020, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.05.005, Available: http://aetic.theiaer.org/archive/v4/v4n5/p5.html.

intelligence in one system segment by disassociating the sending procedure of data packet (Data Plane) from the routing procedure (Control plane). The control plane comprises one or multiple controllers which are considered as the cerebrum of SDN. SDN engineering may empower, encourage, or improve network-related security applications because of the controller's focal perspective of the network system, and its ability to reconstruct the infrastructure plane at any time. Before SDN was started, the objective to make a programmable systems administration framework had for a broad time been considered, for example, the researchers in [1-8], maintained quick programmable information taking care of.

The abilities of SDN, including programming-based [9-14] activity, unified control, centralized view of the system, dynamic refreshing of sending rules, make it less demanding to distinguish and respond to Distributed Denial of Service (DDoS) attack. But the potential DDoS vulnerabilities exist over the SDN platform [15]. DDoS attacks are an endeavour to make a machine or network system's resource inaccessible to its legitimate clients. DDoS attacking traffic is sent by two or many people or using thousands of bots [16]. In order to commence a functional DDoS attack, digital aggressors generally capture a system like PCs or web associated devices, which is familiar as a botnet. The attacker can enrol numerous machines on the grounds that numerous machines are promptly vulnerable [17]. The controllers could possibly be viewed as a single point of failure risk for the whole SDN infrastructure, so is considered an attractive target for DDoS attack [15]. Single controller placement means a single point of control and management of the SDN operation. But there is a high risk to fail the whole network topology as the controller connected to all switches. If the controller become malfunction all the switches connected to that particular controller will be malfunction. So, the legitimate users will not be able to get the services. This is why the controller is the attractive point of attack for the attacker. To avoid this type of devastating single point of failure risk of SDN infrastructure, it is essential to place multiple smart backup controller to ensure the SDN service under DDoS attack. The main benefit of multiple smart backup controllers to keep uninterrupted service for the legitimate user. If the first smart backup controller become overloaded or malfunctioned due to huge DDoS attack traffic, the second or third smart controller will take the responsibility of the victim smart backup (1st) controller illustrated in figure 1. During the support of the 2nd or 3rd smart backup controller, the 1st smart backup controller will be able to refresh and start work again.

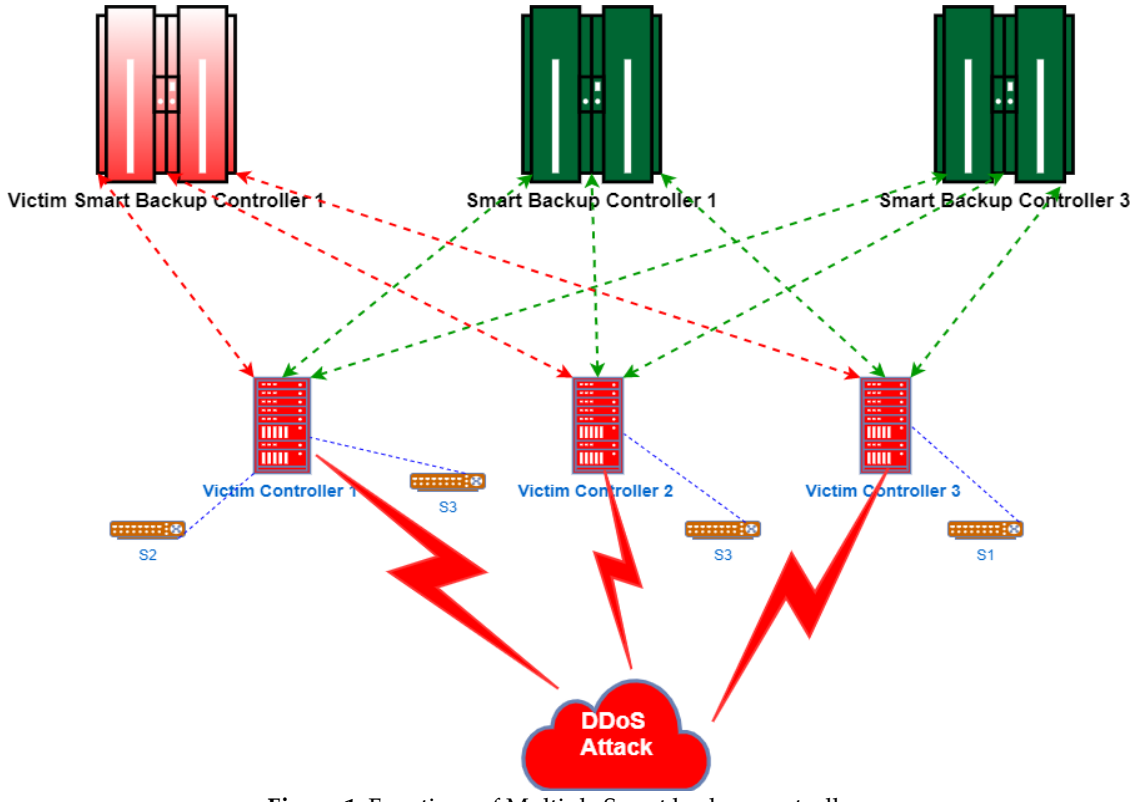

Figure 1. Functions of Multiple Smart backup controllers

The same refresh cycle will work for all smart backup controller vice versa. Thus, the service will be more secured and uninterrupted. But the cost will be higher to place many smart controllers. It is necessary to minimize the total cost. Though a powerful controller is expensive but multiple smart backup controllers can share the maximum new flows per second and port of each other. It will save the cost of the extra controller, extra link, extra bandwidth, and extra manpower. It is suitable where the frequencies of attack are very high. DDoS attacking tools becoming more sophisticated, more frequent, more powerful day by day [18]. It is going very difficult to trace and defend the attacker. Centralized management and programmability are the main features of the SDN controller. So, if the controller fails by an attack it will act as a centralized vast failure. To protect SDN operation from this type of failure we have to place multiple smart backup controllers which is the key point to provide continuous network operation. However, multiple controllers are costly but one powerful backup controller is cheaper in cost. For example, there are different costs for both software and hardware controller. Every software controller must install in a hardware controller. So, if any investor needs 10 software controllers, he must buy 10 hardware controllers to run those controllers. But if there one powerful software controller can install on single powerful hardware controller the cost of 9 software and 9 hardware controllers will be saved. So, if the software controller cost is $6,500 and the hardware controller cost is $5,000, the total cost will be $11,500. For 10 software and 10 hardware controller it will cost 11,500x10 = $115,000. If one powerful controller cost is $30,000 the ultimate savings will be $85,000. The market price varies from vendor to vendor like HP Aruba VAN SDN Controller Base Software with 50-node E-LTU (J9863AAE) $ 9,619 [19] but NEC ProgrammableFlow PF6800 OpenFlow controller is $75,000 [20].

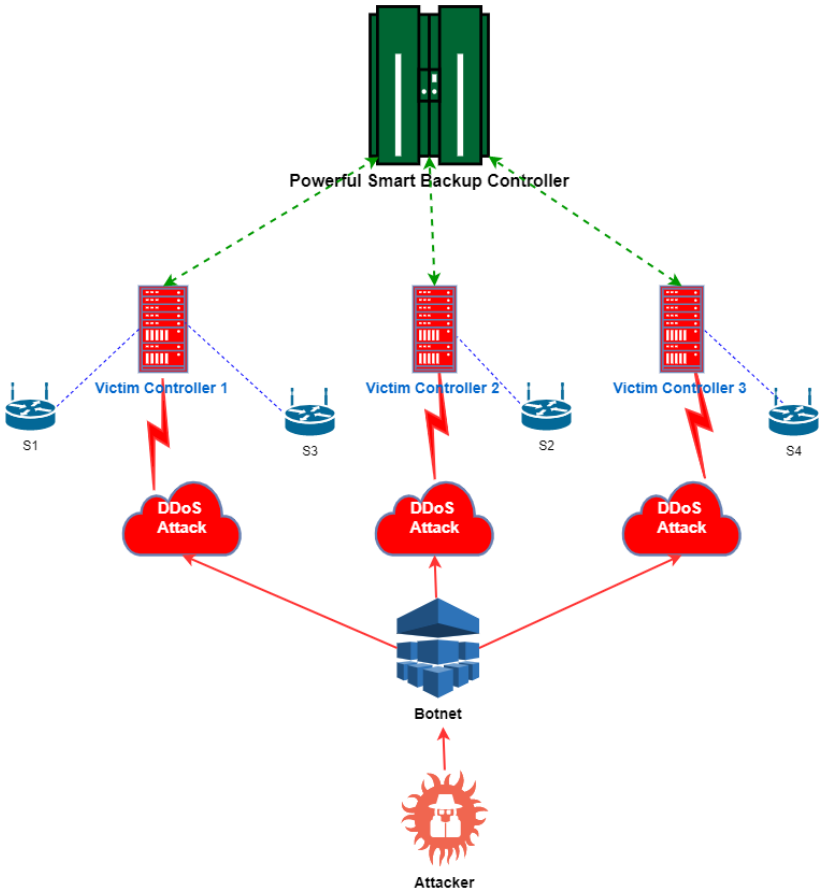

Figure 2. Powerful Smart Backup Controller is supporting multiple ordinary controllers

In Fig. 2 it has been illustrated that a DDoS attacker is sending commands to several controllers via a botnet. Due to the huge number of DDoS traffic [21,22], several controllers have become malfunctioned. But a powerful backup controller takes over the responsibility of victim controllers to provide continuous operation for the legitimate SDN user. To minimize the cost, it is sharing the Maximum new flows per second, port, link bandwidth of the victim controller.

Multiple smart backup controllers will increase the total cost of SDN planning. So how many smart backup controllers need to place and where to place those controllers are critical issues. The Ultimate objective of this paper is to provide continuous SDN service under DDoS attack by placing a smart backup controller during SDN infrastructure planning. The smart backup controller has the capacity to save the cost of multiple controllers by sharing links, Maximum new flows per second, and port. If it is required to place 10 controllers, the investor must pay for 10 links with huge bandwidth, 10 processors or servers, and definitely, huge manpower cost to install. But when one powerful smart controller will share a link, maximum new flows per second by processor and port, so it is saving the extra link cost to multiple controllers, bandwidth cost, and manpower cost-effectively. That's why it is practically cost-effective. As of now, there is no single SDN [23-25] regulator that has the ability to give sufficient conveys security, vigor, and versatility benefits all the while [26].

In section 2 we presented related work. Smart backup controller placement ILP formulation model introduced in section 3. Section 4 contains results and diagram from the proposed model, in section five we furnished future direction and finally, we conclude this paper in section six.

2. Related Works

A static SDN controller placement can't acquire a productive accomplishment in scattered and dynamic networks. A single or haphazard controller placement may not be achievable in Controller Placement Problem (CPP) and careful designing is of the pith to locate a fitting balance among the measurements [27]. In [28] developed a structure that deals with a movement of controller plan issue from crucial to perplexed use cases. To improve the control limit, given a proof-of-thought use of a multi-controller edge structure and measure traffic deferral and overheads. Be that as it may, their results reveal the affectability of deferral to the zone of controllers and the degree among controller and controller center overheads [29]. In [30] thought about the issue of adding some additional controllers to the association to assemble its adaptability to centered attacks. For that, they introduced a special headway model for handling the associated controller circumstance issue. Various controllers furthermore accomplish a couple of troubles where ideal CPP is a customary issue [31-40]. For instance, to ensure network flexibility, it is missing to just grow the number of controllers or aimlessly setting the controllers wherever as an attractive execution can't be refined [37]. This infers different controllers should be suitably situated in fitting zones to meet a couple of necessities and this action included association allotting [31], [39], [41]. In light of everything, allocating association into various control territories to achieve extraordinary association execution can introduce a couple of challenges than predicted with respect to the reliability, load balancing, latency, computation time, etc. [31], [39]. [42] proposed a Steiner tree-based between controller dormancy model, a multi-target number direct program is acquainted with reason the controller position updating (a) synchronization cost in dissatisfaction free circumstances, and, (b) strength against single-interface disillusionment.

[43] proposed that the CPP can be changed into a Controller Selection Problem (CSP). They just select the controller based on the QoS requirement of flow. It's not for the SDN planning stage it's for SDN operational stage: where to forward the data via which controller via a switch. In [44] introduces the utilization of interdependence network analysis to think about the controller placement for network strength, outlines another flexibility metric, and proposes an answer for enhancing versatility. Authors in [45] propose a non-zero-entirety-based diversion theoretic plan which can be utilized as a part of a dispersed way at every dynamic SDN controller. In [46] proposed a controller arrangement technique for a Wide Area Network (WAN), whose goal is to limit the average latency. The focal thought is to parcel the WAN into littler areas by utilizing a spectral clustering algorithm and appoint a controller to every domain. In [47] proposed RTZLK-DAA SDN controller placement Algorithm and ILP model to confront DDoS assaults by setting reinforcement controller at suitable hubs to guarantee the support of authentic SDN clients stayed continuous. But their proposed model cannot support several victim controllers by a powerful smart backup controller. A linear programming model for the layout of controller that restricts the expense of the association with an

upper bound on latency is proposed in [48]. In [49] proposed a methodology that adjusts the number and area of the controllers with changing system conditions. [50] proposed a capacitated next controller arrangement in SDN that maintain a strategic distance from detachments, rehashed regulatory intercession, and extraordinary increment in the most pessimistic scenario inertness if there should arise an occurrence of controller disappointments.

Authors in [51] propose a novel placement metric for sending different controllers that measures the cost when controllers with restricted limit handle ask for messages from switches. [52] Inspects the impact of DDoS attacks on the SDN controller and the way it can debilitate controller resources. In [53] proposed a multi-line SDN controller planning algorithm dependent on the time cut designation procedure identified with regulator arrangement in SDN. By assault traffic, assault scale, and timetables [54] address recognition of DDoS assault in cloud administrations. All things considered, their proposed calculations are the simply link to identify assaults that made the controller glitch which brought about the interferences of administration. [55] Presented pSMART, a lightweight, security-mindful help work chain coordination in a multi-space NFV/SDN circumstance, which can't uphold during the immense volume of DDoS assault traffic. Authors in [56] analyzed various machine learning methods that can be utilized to deal with the issues of interruption and DDoS attacks to SDN. In [57] provided some SDN supported systems against DDoS attack in customary network systems. An efficient review of different SDN self DDoS dangers is then presented. The author in [58] discussed SDN specific centralization creates scalability problems in large network environments. [59] proposed a hypothetical concept of smart controller placement for SDN architecture. [60] Studied the SDN controller circumstance issue for single-interface and multi-associate frustrations, exclusively. For single-interface disillusionments, they developed a heuristic computation to address the controller position issue. For multi-interface disillusionments, the familiar the Monte Carlo Simulation with reducing the computational overhead. Authors in [61] presented a theoretical model of SDN-UAV-EV engineering to execute SDN with Unmanned Aerial Vehicle (UAV) and self-driving Electric Vehicle (EV) utilizing Satellite which is savvy for satellite connection spending plan and SDN design. SDN will apply future applications, for example, voice over IP (VoIP) [62-64]45-47] fibre optic [65-67], overall interoperability for Microwave Access (WiMAX) [68-70] 51-53], Information-Centric Networking (ICN) [71-74] and artificial intelligence (AI) [75]. Authors in [76] analysed the controller placement model to decrease the effect of DDoS attacks, which is created by accepting a speculative network in Malaysia.

The above works neither considered multiple smart backup controllers placement under DDoS attack nor maximum new flows per second and port sharing of multiple smart backup controller to reduce cost.

3. Smart Controller Placement Problem Formulation Model

Five important parameters are, namely,

(1) Number of controllers where each of them may be shared with a smart backup controller based on attack frequency.
(2) The maximum number of packet requests controller or smart backup controller can handle per second.
(3) The range and the bandwidth availability for each link type to be connected between the controllers and the switches.
(4) The quantity of traffic that needs to send from the switch to the controller.
(5) The variety of maximum latency for wireless and copper wire communications.

The following notations are used in the formulation of our proposed SDN model.

3.1. Notation

3.1.1. Sets of the model

$\boldsymbol{B}$ = *{b1, b2, b3, ……}*, set of smart backup controller of type (b∈B) that will be installed if DDoS attack occur on any controller.

λ^b : Number of ports of smart backup controller of type ($b \in B$).

μ^b : Maximum new flows per second of the smart backup controller of type ($b \in B$).

γ^b : Cost of the smart backup controller of type ($b \in B$).

ϱ^b : Different types of the available smart backup controller of type of ($b \in B$) to install.

C = *{c1, c2, c3 …..}*, set of a controller of type of controller (c∈C) that will be installed in SDN with the following property:

λ^c : Number of ports of controller ($c \in$ C).

μ^c : Maximum new flows per second of the controller of type ($c \in$ C).

γ^c : Cost of the controller of ($c \in$ C).

ϱ^c: Different types of the available controller ($c \in C$) to install.

δ = *{s1, s2, s3 …….}*, set of switches type (s∈δ) that will connected to the controller.

- φ^s : The number of available packets that do not match on the switch's ($s \in \delta$) flow table and that are sent to the installed controller to process.

ζ = *{l1, l2, l3….}*, set of Link type of (l∈ζ) connect controller and switch based on:

- ψ^l / Mbps: Bandwidth of the link type ($l \in \zeta$) in byte.

- ω^l / meter Cost of the link of type ($l \in \zeta$) based on the bandwidth type. Cost calculated in US$ per meter.

η = {n1, n2, n3, n4, n5, n6, n7……. nN}, set of the given node where controller are placed.

$DDoS^{\eta}$ = {1, 2, 3…}, set of possible attack on installed controller on node (n∈η). The characterized recurrence of DDoS attacks is going from 0 to 3 where 0 speaks to no assault. 1, 2, 3 mean low, medium, high recurrence of attack separately. The model will place the savvier backup controller in the accompanying situations:

(1) Network activities that require high accessibility, for example, military, medical, banking, and data center. or then again/and

(2) Those nodes which encountering a higher recurrence of the attack.

3.1.2. Constants

$\theta^{c/b}$**:** Packet size in byte to be processed via controller type of ($c \in$ C) or smart backup controller type of ($b \in B$).

ξ **:** Speed of light to calculate the latency in wireless communication.

Range^{ab}: The space between two places 'a' to 'b'. It's the space between either two controllers, controller to switch or smart backup controller to ordinary controller.

π **:** Function to convert Mbps or Gbps in byte.

$\kappa^{c \text{ and } b}$Processing time for the controller type of ($c \in$ C) and smart backup controller type of ($b \in B$).

$\nu^{(\text{WirelessCom})}$**:** Maximum allowable latency using wireless communication.

$\nu^{(\text{CopperWireCom})}$: Maximum latency using copper wire communication.

3.1.3. Decision Variables of the SDN Model under DDoS attack

T_{cn} : 1, only in the case of when, the model placed a controller (c∈C) at node (n∈η), all other cases 0.

T_{bn}**:** 1, only in the case of when, the model placed a smart backup controller of type (b∈B) at sharing node (n1∈η or n2∈η etc), all other cases 0.

Z^l_{sn}**:** 1, only in the case of when, a link (l∈ζ) is associated between switches type of (s∈δ) and the model placed a controller on the node (n∈η), all other cases 0.

R^l_{nm}**:** 1, only in the case of when, a controller location (n∈η) is associated to the controller location (m∈η) with a link type (l∈ζ), all other cases 0

R^l_{cb}**:** 1 if multiple controller (c1∈C, c2∈C, etc) are connected to Smart Backup Controller (b∈B) with multiple links type (l∈ζ), all other cases 0.

3.2. Cost Functions

The objective of this mathematical model is to minimize the total cost of SDN by placing multiple smart backup controller, which will share the Maximum new flows per second of multiple controllers under DDoS attacks. Cost depends on the number and types of the controller ($Cost^c$ (T^c)) installed in

SDN, smart backup controller placement respect to the number and frequency of DDoS Attack (Cost^{b} (T^{b})), and type of link connected controller to controller (Cost^{ζ} (R)) and switches to the controller (Cost^{ζ}(Z)) and Cost^{ζ} (R^b) link between controller to the smart backup controller in SDN.

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

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

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

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

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

3.3. The SDN Model

The number of the required smart backup controller depends on the availability of network requirements and the probability of frequency of DDoS attacks on the SDN controller. The mathematical model for the DDoS attack-aware smart backup controller placement planning can be modelled as follows.

3.3.1. Objective Function

Minimize

$$\mathbf{Cost}^{\text{c}}\ (\mathbf{T}^{\text{c}}) + \mathbf{Cost}^{\text{b}}(\mathbf{T}^{\text{b}}) + \mathbf{Cost}^{\zeta}(\mathbf{Z}) + \mathbf{Cost}^{\zeta}\ (\mathbf{R}) + \mathbf{Cost}^{\zeta}\ (\boldsymbol{R^b})$$

3.3.2. Subject To

$$\sum_{b\in \boldsymbol{B}}\mathbf{T_{bn}}\ \geq\ \mathbf{DDoS}^{\boldsymbol{n}}\ \ (\boldsymbol{b}\in \boldsymbol{B}, \boldsymbol{n}\in \boldsymbol{\eta}) \tag{6}$$

$$\sum_{c\in \text{C}}\boldsymbol{\mu^{cn}}\,\mathbf{T}_{\boldsymbol{cn}} + \sum_{c\in \text{C}}\ \boldsymbol{\mu^{co}}\,\mathbf{T}_{\boldsymbol{co}}\ \leq\ \sum_{b\in \text{B}}\ \boldsymbol{\mu^{b}}\,\mathbf{T_{b\eta}}(\boldsymbol{n}\in \boldsymbol{\eta}) \tag{7}$$

$$\sum_{c\in \text{C}}\boldsymbol{\lambda^{cn}}\,\mathbf{T}_{\boldsymbol{cn}} + \sum_{c\in \text{C}}\ \boldsymbol{\lambda^{co}}\,\mathbf{T}_{\boldsymbol{co}}\ \leq\ \sum_{b\in \text{B}}\ \boldsymbol{\lambda^{b}}\,\mathbf{T_{b\eta}}(n\in \eta) \tag{8}$$

The above constraint (6) is calculating the frequency of attack or number of attacks to place a powerful smart backup controller.

This constraint (7) will ensure the powerful backup controller's Maximum new flows per second is higher than the number of the affected controller. It will share the backup controller's Maximum new flows per second to another backup controller.

Powerful backup controller's port is sufficient enough to support multiple affected controller's ports. Constraint (8) is essential to share the backup controller's port with another backup controller's port.

$$\sum_{b\in \text{B}}\ \boldsymbol{\mu^{b}}\,\mathbf{T_{b\eta}}\geq\ \sum_{c\in \text{C}}\boldsymbol{\mu^{c}}\,\mathbf{T}_{\boldsymbol{cn}}(n\in \eta) \tag{9}$$

The Backup controller's maximum new flows per second must be more than the affected controller.

$$\sum_{b\in \text{B}}\ \sum_{n\in \eta}\ \mathbf{T_{b\eta}}\geq\ \mathbf{T_{b\eta}}(b\in B, n\in \eta\ ) \tag{10}$$

Multiple backup controllers will install if it is necessary on any node based on maximum new flows per second and port.

$$\sum_{\mathbf{l}\epsilon \mathbf{L}}\ \boldsymbol{R_{cb}^{l}} =\ \ \mathbf{T_{bn}}\ (n\in \eta, b\in B\ ) \tag{11}$$

Exactly one link via wired or wireless communication will ensure the communication between the controller and backup controller under DDoS attack.

Next, the latency of the backup controller varies from wireless communication to copper wire communication. Latency also varies for the range of two nodes of SDN. The maximum latency of the backup controller must be smaller than the required latency.

$$\frac{\mathbf{2\theta^{b}}}{\boldsymbol{\psi^{l}}}\boldsymbol{Z_{sn}^{l}} + \sum_{b\in B}\ \frac{\mathbf{2Range^{cb}}}{\boldsymbol{\xi}}\mathbf{T_{b\eta}} +\ \boldsymbol{\varphi^{s}}\mathbf{T_{b\eta}}\leq\ \boldsymbol{\nu}(n\in \eta, s\in \delta, l\in \zeta\ ) \tag{12}$$

The maximum latency of the controller must be smaller than the required latency. The latency for the controller also varies from wireless communication to copper wire communication.

The number of backup controller placements shall be not more than the number of inventories of backup controllers.

$$\sum_{b\in B} \mathbf{T_{bn}} \leq \boldsymbol{\rho^b}(n \in \eta) \quad (13)$$

The model will check the availability of the controller before placement using this constraint.

$$\sum_{c\in C} \mathbf{T_{cn}} \leq \boldsymbol{\rho^c}\ (n \in \eta) \quad (14)$$

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

$$\sum_{c\in C} \mathbf{T_{cn}} \leq \mathbf{1}\ (n \in \eta) \quad (15)$$

A controller is connected to a switch with only one link.

$$\sum_{l\in\zeta} \sum_{n\in\eta} \boldsymbol{Z^l_{sn}} = \mathbf{1}\ (s \in \delta) \quad (16)$$

A fully connected network or complete topology will be the topology for this SDN. It depends on the SDN planner. It will connect the controller to the controller [11].

$$\sum_{c\in C} \mathbf{T_{cm}} + \sum_{c\in C} \mathbf{T_{cn}} \leq \sum_{l\in\zeta} \boldsymbol{R^l_{nm}} + \mathbf{1}\ (n \in \eta, m \in \eta, m > n) \quad (17)$$

The following constraint ensures that the number of switch and controller must be less than the available port on the controller.

$$\sum_{\mathbf{m}\epsilon\eta} \sum_{l\in\zeta} \left(\boldsymbol{R^l_{nm}} + \boldsymbol{R^l_{mn}}\right) + \sum_{s\in\delta} \sum_{l\in\zeta} \boldsymbol{Z^l_{sn}} \leq \sum_{c\in C} \boldsymbol{\lambda^c}\, \mathbf{T_{cn}}\ (n \in \eta) \quad (18)$$

The bandwidth of the link must be available based on the required bandwidth in order to communicate between switch and controller. This constraint will convert the data packets into bytes.

$$\sum_{s\in\delta} \boldsymbol{\varphi^s \theta^{c/b}} \geq \sum_{c\in C} \boldsymbol{\pi}\ \boldsymbol{\psi^l Z^l_{s\eta}}\ (n \in \eta) \quad (19)$$

The following constraint will check the maximum new flows per second of the controller to handle the data from switches.

$$\sum_{l\in\zeta} \sum_{s\in\delta} \boldsymbol{\varphi^s}\, \boldsymbol{Z^l_{s\eta}} \leq \sum_{c\in C} \boldsymbol{\mu^c}\, \mathbf{T_{c\eta}}\ (n \in \eta) \quad (20)$$

The data used in the computation are tabulated in Table 1, Table 2, Table 3, Table 4, Table 5, and Table 6. The cost of the controller, backup controller, and bandwidth are hypothetical (average) because there are many different vendors such as HP Aruba VAN SDN Controller[1], Huawei Agile Controller[2], Cisco Open SDN Controller[3], etc. with different pricing. with the input data from.

Table 1. Controller Type and Parameters

Controller Type	λ^c	μ^c	γ^c	ϱ^c
C1	8	7250	$4000	20
C2	32	8000	$7500	15
C3	24	9000	$5419	10

Table 2. Powerful Smart Backup Controller Type and Parameters

Smart Backup Controller Type	λ^b	μ^b	γ^b	ϱ^b
BC 1	72	4500	$3750	2
BC 2	50	18000	$7800	2
BC 3	12	15000	$8450	2

Table 3. Type of Link and Cost

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

Table 4. Switch Types and Data Size

Switch type	φ^s
S1	2000
S2	8000
S3	7000

Table 5. Other Constant Data

Constant Type	Data
$\theta^{c/b}$	500 byte
ξ	299792458 m/s
$\boldsymbol{Range^{\delta\eta}}$	100m

[1]HP Aruba VAN SDN Controller, https://marketplace.hpe.com/ (accessed on 07 July 2020).
[2]Huawei Agile Controller, http://itprice.com/huawei/agile-controller-56/ (accessed on 07 July 2020).
[3]Cisco Open SDN Controller, https://www.cisco.com/c/en/us/support/cloud-systems-management/open-sdn-controller/series.html (accessed on 07 July 2020).

$Range^{m\eta}$	100m
$Range^{cb}$	1m
π	1/8
$\kappa^{c \text{ and } b}$	0.000001 ms
$\nu^{(WirelessCom)}$	10,000 ms
$\nu^{(CopperWireCom)}$	300000000000 ms

4. Experimental Results and Discussion

Our proposed novel model has been developed using A Mathematical Programming Language[4] (AMPL), it underpins formulation, simulation and development, and IBM ILOG CPLEX[5] with Intel (R) core (TM) i7–6700 CPU@3.40GHz, RAM 8GB and virtual memory 128GB machine. Our proposed model is evaluated in several different scenarios. In Table 6, we present five different most representative scenarios.

The proposed model is evaluated under several frequencies of DDoS attack. We are presenting the 5 different DDoS attack scenarios as shown in Table 6. First column is for the scenario serial number. Second column for switches (δ), Third column for links (ζ), Fourth column for Input nodes (Iη) and nodes (η), Fifth column for controllers (C), Sixth column for available data packet per second need to process by controller, seventh column represents the frequency of DDoS attack types such as low, medium, high attacks. The last three columns represent the obtained simulation results from all various scenario in term of victim controller, the number of powerful backup controller placement and total SDN cost in US$ respectively.

Table 6. CPLEX Solutions: Smart Backup Controller placement under DDoS attack on controller

S#	δ	ζ	Iη / η	C	Packets per Second	Frequency of Attack	Victim Controller, μ^c and λ^c	Smart Backup Controller, μ^b and λ^b	Cost (US$)
1	3	6	9/2	2	17,000	Two Single attack (1,1) at N8 (C3-1a) and N9 (C3-1a)	2 (C3-1a, C3-1a), (9000 + 9000 = 18000), (24 + 24 = 48)	(BC2), 18000, 50	26,688.5
2	3	7	9/2	2	17,000	One single attack and one double attack (1,2) at N8 (C3-1a) and N9 (C3-2a)	2 (C3-1a, C3-2a), (9000 + 9000 = 18000), (24 + 24 = 48)	(BC1), 4500, 72 (BC2), 18000, 50	30,438.75
3	3	8	9/2	2	17,000	Two double attack (2,2) at N8 (C3-2a) and N9 (C3-2a)	2 (C3-2a, C3-2a), (9000 + 9000 = 18000), (24 + 24 = 48)	(BC1), 4500, 72 (BC2), 18000, 50	34,189
4	3	8	9/2	2	17,000	One single attack and three triple attack (1,3) at N8 (C3-1a) and N9 (C3-3a)	2 (C3-1a, C3-3a), (9000 + 9000 = 18000), (24 + 24 = 48)	(BC1), 4500, 72 (BC2), 18000, 50 (BC3), 15000, 12	38,889
5	3	10	9/2	2	17,000	Three triple attack (3,3) at N8 (C3-3a) and N9 (C3-3a)	2 (C3-3a, C3-3a), (9000 + 9000 = 18000), (24 + 24 = 48)	1 (BC1), 4500, 72 2 (BC2), 18000, 50 3 (BC3), 15000, 12	51,089.5
The total cost included controllers, Powerful Smart backup controllers, bandwidth, and link's cost.									

4.1. Scenario 1

In the second row of Table 6, the input node (Gη) was 9, implying 9 controllers shall be deployed at 9 nodes. However, the optimization from our model proposed 2 nodes (η) with 2 controllers (C), 3 switches (δ), and 6 links (ζ). This result demonstrated a saving of 1 controller and 7 nodes in total. The total available data packet per second was 17,000, which can process by 2 controllers. Two Single attacks (1,1) at N8 (C3-1a) and N9 (C3-1a) has occurred. The Maximum new flows per second of 2 controller are (C3-1a, C3-1a), (9000 + 9000 = 18000 packet per second-PPS), and the port are (24 + 24 = 48). So, the model recommended 1 powerful backup controller (BC2) with 18000 PPS Maximum new flows per second and 50 port. Which can support the victim controllers easily.

[4]A Mathematical Programming Language (AMPL), https://ampl.com/ (accessed on 09 Nov 2020).
[5]IBM ILOG CPLEX Optimization Studio, https://www.ibm.com/products/ilog-cplex-optimization-studio (accessed on 03 Oct 2020).

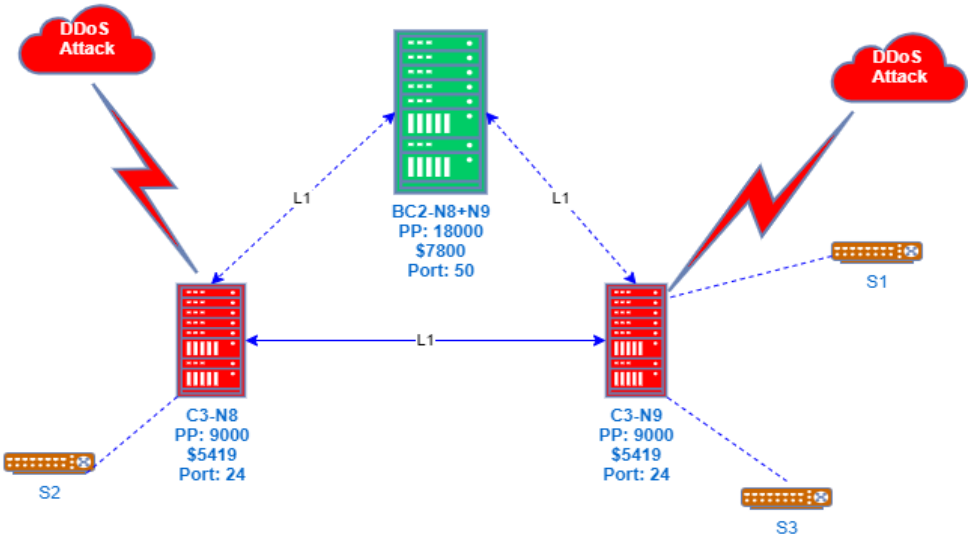

Figure 3. Diagram from the scenario 1

4.2. Scenario 2

Represents in the third row from Table 6 the input node (Gη) was 9, implying 9 controllers shall be deployed at 9 nodes. However, the optimization from our model proposed 2 nodes (η) with 2 controllers (C), 3 switches (δ), and 6 links (ζ). This result demonstrated a saving of 1 controller and 7 nodes in total. The total available data packet per second was 17,000, which can process by 2 controllers. One single attack and one double attack (1,2) at N8 (C3-1a) and N9 (C3-2a) have occurred. The Maximum new flows per second of 2 controller are (C3-1a, C3-1a), (9000 + 9000 = 18000 packet per second-PPS), and the port are (24 + 24 = 48). So, the model recommended two backup controllers, 1 powerful backup controller (BC2) with 18000 PPS Maximum new flows per second and 50 port, and 1 backup up the controller (BC1) with 4500 PPS and 72 ports. Which can support the victim controllers affected by 2 different (one high and one medium) frequencies of DDoS attack.

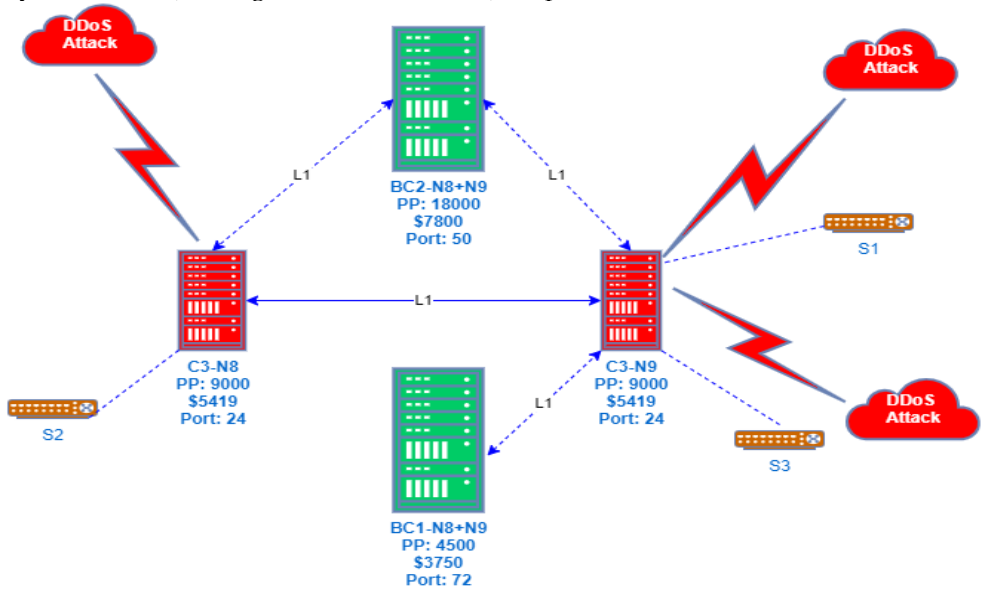

Figure 4. Diagram from the scenario 2

4.3. Scenario 3

The input node (Gη) was 9, implying 9 controllers shall be deployed at 9 nodes. However, the optimization from our model proposed 2 nodes (η) with 2 controllers (C), 3 switches (δ), and 6 links (ζ). This result demonstrated a saving of 1 controller and 7 nodes in total. The total available data packet per second was 17,000, which can process by 2 controllers. Two double attacks (2,2) at N8 (C3-2a) and N9 (C3-2a) has occurred. The Maximum new flows per second of 2 controllers are (C3-2a, C3-

2a), (9000 + 9000 = 18000 packet per second-PPS), and the port are (24 + 24 = 48). So the model recommended 2 backup controllers, 1 powerful backup controller (BC2) with 18000 PPS Maximum new flows per second and 50 port and 1 backup controller (BC1) with 4500 PPS and 72 ports. Which can support the victim controllers affected by 2 different medium frequencies of DDoS attack.

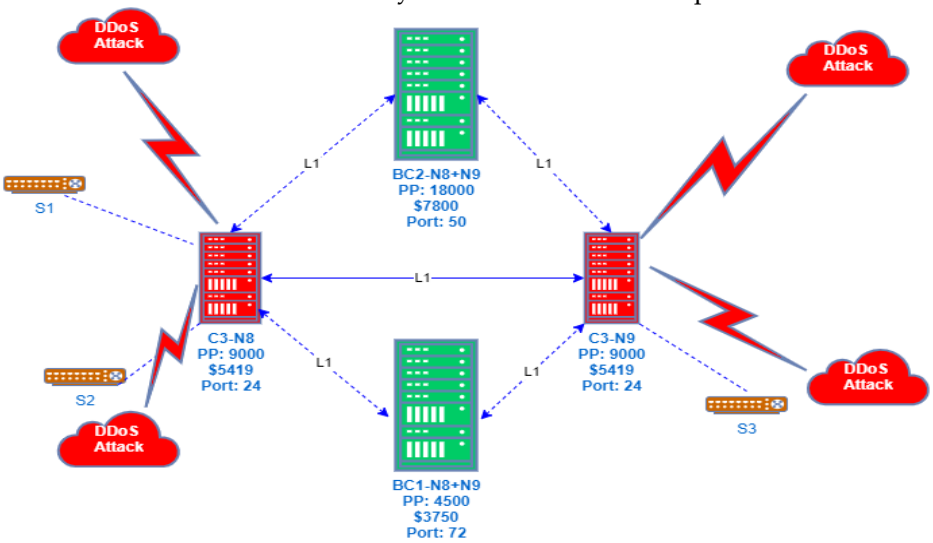

Figure 5. Diagram from the scenario 3

4.4. Scenario 4

The input node (Gη) was 9, implying 9 controllers shall be deployed at 9 nodes. However, the optimization from our model proposed 2 nodes (η) with 2 controllers (C), 3 switches (δ), and 6 links (ζ). This result demonstrated a saving of 1 controller and 7 nodes in total. The total available data packet per second was 17,000, which can process by 2 controllers. One single attack and three triple attacks (1,3) at N8 (C3-1a) and N9 (C3-3a) has occurred. The Maximum new flows per second of 2 controller are (C3-2a, C3-2a), (9000 + 9000 = 18000 packet per second-PPS), and the port are (24 + 24 = 48). So the model recommended 3 backup controllers, 1 backup controller (BC1) with 4500 PPS and 72 ports, 1 powerful backup controller (BC2) with 18000 PPS Maximum new flows per second and 50 port, and 1 powerful backup controller (BC3) with 15000 PPS and 12 port. Which can support the victim controllers affected by 3 different (one single and 3 very high) frequencies of DDoS attack.

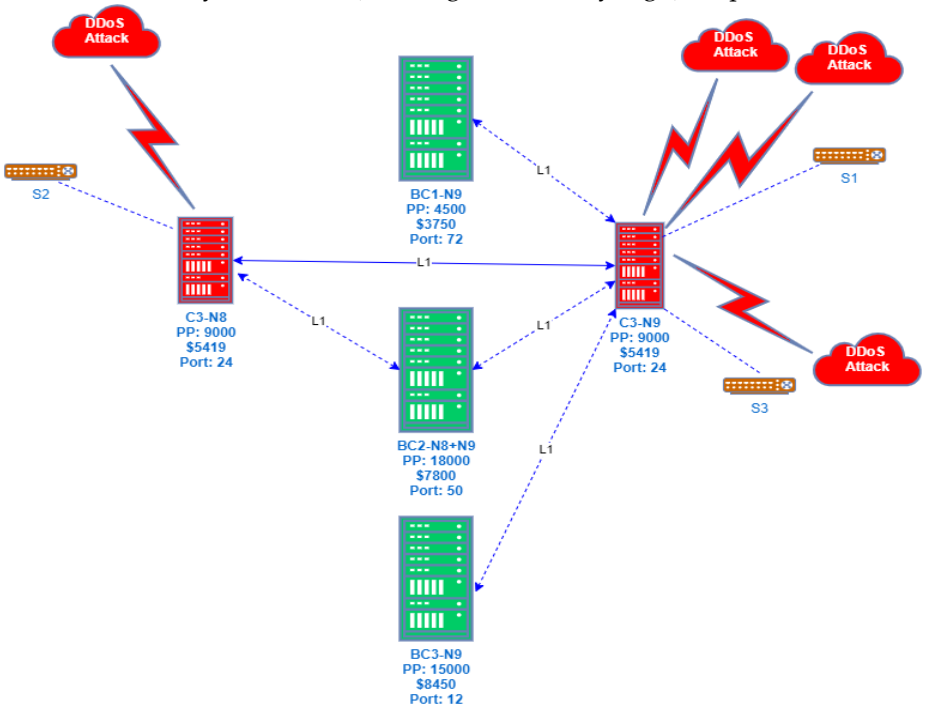

Figure 6. Diagram from the scenario 4

4.5. Scenario 5

Finally, the input node (Gη) was 9, implying 9 controllers shall be deployed at 9 nodes. However, the optimization from our model proposed 2 nodes (η) with 2 controllers (C), 3 switches (δ), and 6 links (ζ). This result demonstrated a saving of 1 controller and 7 nodes in total. The total available data packet per second was 17,000, which can process by 2 controllers. Three triple attacks (3,3) at N8 (C3-3a) and N9 (C3-3a) has occurred. The Maximum new flows per second of 2 controller are (C3-2a, C3-2a), (9000 + 9000 = 18000 packet per second-PPS), and the port are (24 + 24 = 48). So the model recommended 3 backup controllers, 1 backup up the controller (BC1) with 4500 pps and 72 ports, 1 powerful backup controller (BC2) with 18000 pps Maximum new flows per second and 50 port and 1 powerful backup controller (BC3) with 15000 pps and 12 port. Which can support the victim controllers affected by 3 very high frequencies of DDoS attacks.

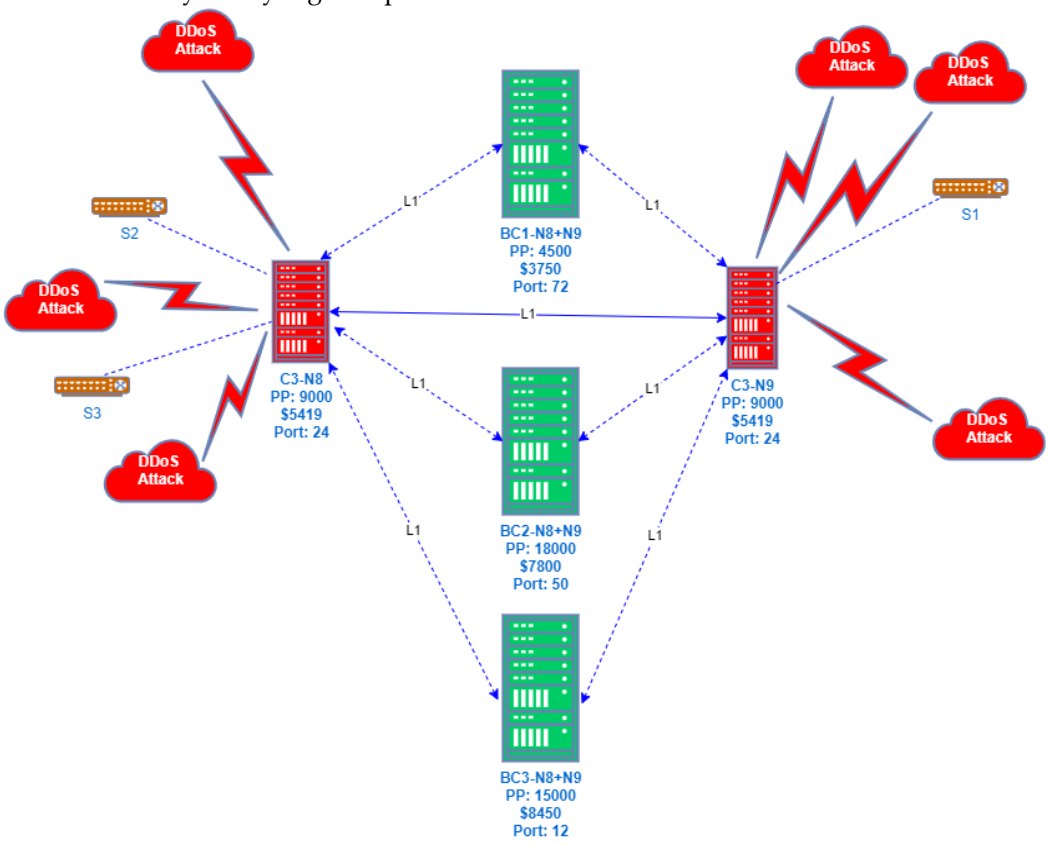

Figure 7. Diagram from the scenario 5

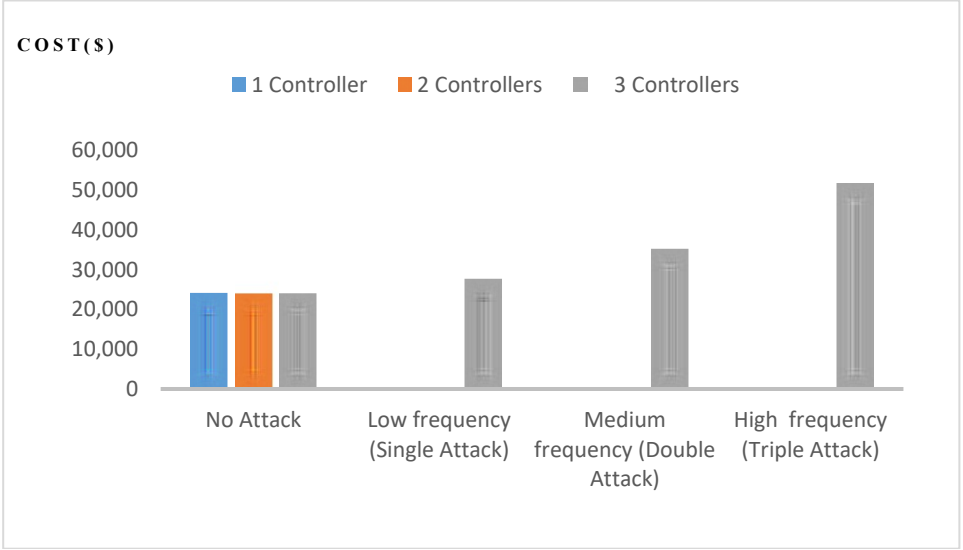

Figure 8. Cost for various recurrence of DDoS assault on the various victim controller

5. Future Direction

Our proposed model is Feasible for planning and deployment in real networking topology for any GEO Location. We are outfitting charts and constant information for IBM (USA) from the Internet Topology Zoo[6].

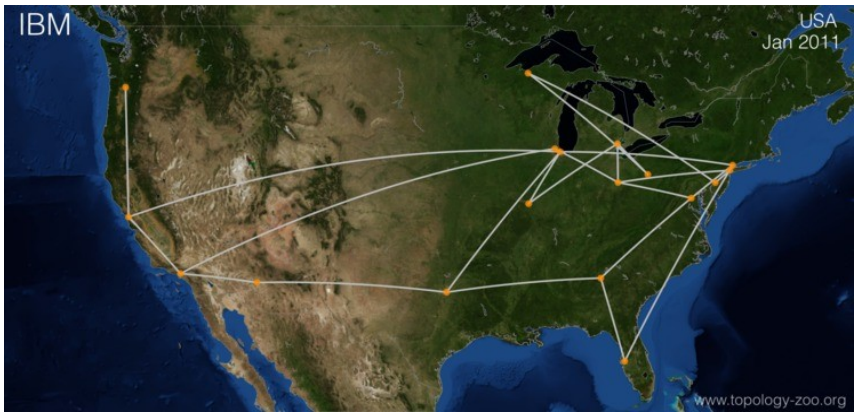

Figure 9. Real time network topology of IBM (USA) from satellite[6]

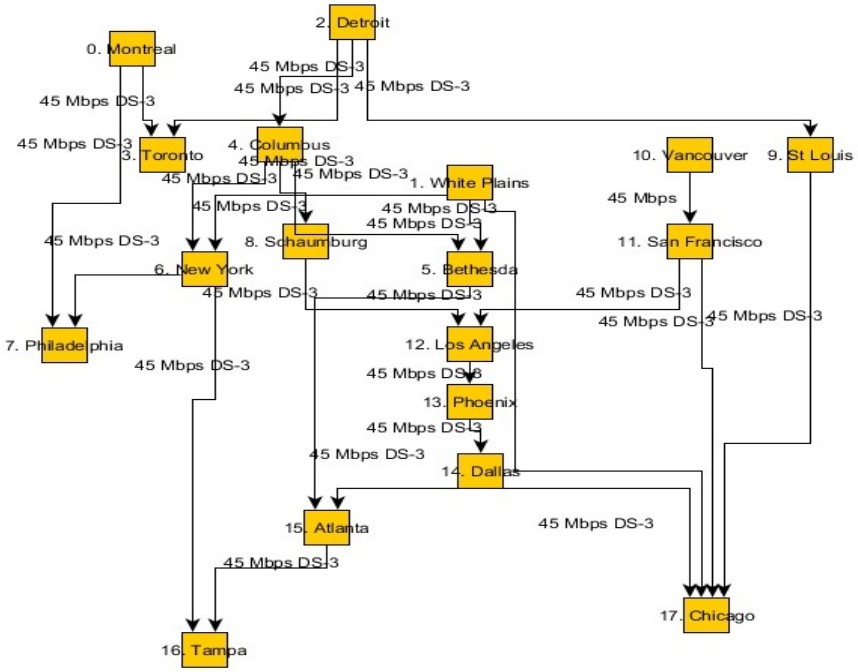

Figure 10. Real topology diagram of IBM (USA)[7].

Table 7. Converted data from the above diagrams of IBM (USA) using yEd[8]

Network	IBM
Number of nodes	18
Router/Switches	18
Number of Edges	24
Longitude	-90.19789 (St Louis)
Latitude	38.62727
Bandwidth	45 Gbps

6. Conclusion

The emerging novel way to deal with cloud computing, data center, and telecommunication network in smart cities is Software-Defined Networking (SDN). But unfortunately, it has to face

[6]The Internet Topology Zoo, http://www.topology-zoo.org/dataset.html (accessed on 03 Nov 2020).
[7]Dataset, http://www.topology-zoo.org/dataset.html (accessed on 03 Nov 2020).
[8]yEd, https://www.yworks.com/products/yed (accessed on 03 Nov 2020).

security issues like DDoS attacks due to its programmability of the controller. Attackers are taking this advantage to malfunction the controller. The Ultimate goal of this paper is to optimize the SDN security issue by placing single and multiple powerful smart backup controllers to support several ordinary victim controllers to minimize the total cost of SDN during planning. In this paper, we proposed a novel Integer Linear Programming (ILP) model to optimize the security issue. Result acquired from simulation demonstrates that our proposed ILP model can recommend powerful smart backup controller which has the ability to spare the cost of numerous controllers by sharing connection (link), maximum new flows per second and port. So, it is saving the extra association cost to various controllers, information exchange limit cost, and manpower cost-effectively. This model is suitable for small and medium scale SDN planning. In the future, we will execute our proposed model with a couple of more boundaries, for example, Artificial Intelligence (AI) capacities, Internet of Things (IoT) devices network, Cloud Computing and DevOps, and information losses, etc.

References

[1] K. Nisar, E. R. Jimson, M. Hijazi and S. K. 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, eISSN: 2635-635X, Available: http://jieta.org/v2n101/ (accessed on 09 Dec 2020).

[2] 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 (IJICTHD)*, Vol, 10, No.4, pp 44-60, 2018, Available: https://doi.org/10.4018/IJICTHD.2018100 (accessed on 09 Oct 2020).

[3] R. di Lallo, F. Griscioli, G. Lospoto, H. Mostafaei, M. Pizzonia and M. Rimondini, "Leveraging SDN to monitor critical infrastructure networks in a smarter way", *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Lisbon, 2017, pp. 608-611.

[4] 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*, August, 2010, Available: https://doi.org/10.1145/1851275.1851206 (accessed on 09 March 2020).

[5] 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, Available: https://doi.org/10.1109/ACCESS.2017.2666200 (accessed on 09 April 2020).

[6] X. Jia, Y. Jiang and Z. Guo, "Incremental Switch Deployment for Hybrid Software-Defined Networks", *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, Dubai, pp. 571-574, 2016.

[7] J. Yang, Z. Yao, B. Yang, X. Tan, Z. Wang and Q. Zheng, "Software-Defined Multimedia Streaming System Aided By Variable-Length Interval In-Network Caching", *IEEE Transactions on Multimedia*, vol. 21, no. 2, pp. 494-509, Feb 2019, Available: https://doi.org/10.1109/TMM.2018.2862349 (accessed on 09 Nov 2020).

[8] S. Han, K. Jang, K. Park and S. Moon, "PacketShader: a GPU-Accelerated Software Router", *ACM SIGCOMM Computer Communication Review*, pp. 1–12, August 2010.

[9] K.Nisar, E. R. Jimson, M. H. A. Hijazi, I. Welch, R.Hassan, A. H. M. Aman, A. H.n Sodhro, S. Pirbhulal and S. Khan, "A Survey on the Architecture, Application, and Security of Software Defined Networking: Challenges and Open Issues", *Internet of Things*, Elsevier, 2020.

[10] K.Nisar, E. R. Jimson, M.Hanafi and S.K. Memon, "Software Defined Network and Comparison of the Throughput Performance with Traditional Network", *Journal of Industrial Information Technology and Application*, eISSN: 2586-0852, vol. 3, No. 4, pp. 298-310, 2019. Available: http://jiita.org/v3n402/ (accessed on October 2020).

[11] 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 (IJICTHD)*, vol. 10, No.4, pp 44-60, 2018, Available: https://doi.org/10.4018/IJICTHD.2018100104 (accessed on November 2020).

[12] K. Nisar, G. Chen and A. Sarrafzadeh, "A Review: Software-Defined Networking Implementation and Testing", *Proceedings of the Asia-Pacific Advanced Network 2015 (APAN)*, Network Research Workshop, Fukuoka, Japan, vol. 39, pp. 1-09, March 01 - 06, 2015, Available: https://doi.org/10.7125/APAN.39.2 (accessed on September 2020).

[13] N. F. Ali, A. M. Said, K. Nisar and I. A. Aziz, "A survey on software defined network approaches for achieving energy efficiency in wireless sensor network", *2017 IEEE Conference on Wireless Sensors (ICWiSe)*, Miri, pp. 1-6, , 2017, Available: https://doi.org/10.1109/ICWISE.2017.8267157 (accessed on October 2020).

[14] E. R. Jimson, K. Nisar and M. H. bin Ahmad Hijazi, "Bandwidth management using software defined network and comparison of the throughput performance with traditional network", *2017 International*

Conference on Computer and Drone Applications (IConDA), Kuching, pp. 71-76, 2017, Available: https://doi.org/10.1109/ICONDA.2017.8270402 (accessed on October 2020).

[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, Firstquarter, 2016, Available: https://doi.org/10.1109/COMST.2015.2487361 (accessed on 6 June 2019).

[16] S. S. Silva, R. M. Silva, R. C. Pinto and R. M. Salles, "Botnets: A survey", *Computer Networks*, vol. 57, no. 2, pp. 378–403, Feb. 2013.

[17] M. R. Haque *et al.*, "Motivation of DDoS Attack-Aware in Software Defined Networking Controller Placement", *2017 International Conference on Computer and Applications (ICCA)*, Doha, pp. 36-42, 2017. Available: https://doi.org/10.1109/COMAPP.2017.8079751 (accessed on 7 June 2020).

[18] radware, "Cloud DDoS Protection Service", Available: https://www.radware.com/products/cloud-ddos-services/ (accessed on 27 June 2018).

[19] Hewlett Packard Enterprise, "Aruba VAN SDN Controller High Availability E-LTU", 2018, Available: https://buy.hpe.com/pdp?prodNum=J9865AAE&country=US&locale=en (accessed 12 March 2019).

[20] R.G. Little, "NEC slashes OpenFlow prices with a $3,000 SDN starter pack", TechTarget, 2018, Available: https://searchsdn.techtarget.com/news/2240232731/NEC-slashes-OpenFlow-prices-with-a-3000-SDN-starter-pack (accessed on 12 July 2019).

[21] K.S. Sahoo, S.K. Panda, S. Sahoo, B.Sahoo and R. Dash, "Toward secure software-defined networks against distributed denial of service attack", *The Journal of Supercomputing*, 75, 4829–4874, 2019, Available: https://doi.org/10.1007/s11227-019-02767-z (accessed on 09 Oct 2020).

[22] K. S. Sahoo et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks", *IEEE Access*, vol. 8, pp. 132502-132513, 2020, Available: https://doi.org/10.1109/ACCESS.2020.3009733 (accessed on 01 Dec 2020).

[23] A. Shirmarz and A. Ghaffari, "Performance issues and solutions in SDN-based data center: a survey", *The Journal of Supercomputing*, Available: https://doi.org/10.1007/s11227-020-03180-7 (accessed on 13 Feb 2020).

[24] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey", *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, Jan 2015, Available: https://doi.org/10.1109/JPROC.2014.2371999 (accessed on 13 Feb 2020).

[25] M. Karakus and A. Durresi, "Quality of Service (QoS) in software defined networking (SDN): a survey", *Journal of Networks and Computer Applications*, 80:200–218, 2017.

[26] Scott-Hayward, S., Natarajan, S., and Sezer, S. "A Survey of Security in Software Defined Networks", *IEEE Communications Surveys and Tutorials*, 18(1), 623-654, 2016.

[27] B. Isong, R. R. S. Molose, A. M. Abu-Mahfouz and N. Dladlu, "Comprehensive Review of SDN Controller Placement Strategies", *IEEE Access*, vol. 8, pp. 170070-170092, 2020, Available: https://doi.org/10.1109/ACCESS.2020.3023974 (accessed on 11 Dec 2020).

[28] Tran, A.K., Piran, M.J. and Pham, C. "SDN Controller Placement in IoT Networks: An Optimized Submodularity-Based Approach", *Sensors*, 19, 5474, 2019, Available: https://doi.org/10.3390/s19245474

[29] Q. Qin, K. Poularakis, G. Iosifidis and L. Tassiulas, "SDN Controller Placement at the Edge: Optimizing Delay and Overheads", *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Honolulu, HI, pp. 684-692, doi: 10.1109/INFOCOM.2018.8485963, 2018.

[30] E. Calle, S. G. Cosgaya, D. Martínez and M. Pióro, "Solving The Backup Controller Placement Problem In SDN Under Simultaneous Targeted Attacks", *2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM)*, Nicosia, Cyprus, pp. 1-7, 2019.

[31] M. Khorramizadeh and V. Ahmadi, "Capacity and load-aware softwaredefined network controller placement in heterogeneous environments", *Computer Communications*, vol. 129, pp. 226–247, Sep 2018, Available: https://doi.org/10.1016/j.comcom.2018.07.037 (accessed on 11 Dec 2020).

[32] K. S. Sahoo, D. Puthal, M. S. Obaidat, A. Sarkar, S. K. Mishra and B. Sahoo, "On the placement of controllers in software-Defined-WAN using meta-heuristic approach", *Journal of Systems and Software*, vol. 145, pp. 180–194, Nov 2018, Available: https://doi.org/10.1016/j.jss.2018.05.032 (accessed on 15 Nov 2020).

[33] A. A. Ateya, A. Muthanna, A. Vybornova, A. D. Algarni, A. Abuarqoub, Y. Koucheryavy and A. Koucheryavy, "Chaotic salp swarm algorithm for SDN multi-controller networks", *Engineering, Science and Technology*, vol. 22, no. 4, pp. 1001–1012, Aug 2019, Available: https://doi.org/10.1016/j.jestch.2018.12.015 (accessed on 15 Dec 2020).

[34] T. Das and M. Gurusamy, "Resilient controller placement in hybrid SDN/legacy networks", *Proceedings of the IEEE Global Communication Conference (GLOBECOM)*, pp. 1–7, Dec 2018, Available: https://doi.org/10.1109/GLOCOM.2018.8647566 (accessed on 15 Dec 2020).

[35] S. Wu, X. Chen, L. Yang, C. Fan and Y. Zhao, "Dynamic and static controller placement in software-defined satellite networking", *Acta Astronautica*, vol. 152, pp. 49–58, Nov 2018.

[36] B. Zhang, X. Wang, and M. Huang, "Multi-objective optimization controller placement problem in Internet-oriented software defined network", *Computer Communication*, vol. 123, pp. 24–35, Jun 2018, Available: https://doi.org/10.1016/j.comcom.2018.04.008 (accessed on 15 Dec 2020).

[37] F. J. Ros and P. M. Ruiz, "On reliable controller placements in softwaredefined networks", *Computer Communication*, vol. 77, pp. 41–51, Mar 2016, Available: https://doi.org/10.1016/j.comcom.2015.09.008 (accessed on 15 Dec 2020).

[38] J. Liao, H. Sun, J. Wang, Q. Qi, K. Li and T. Li, "Density cluster based approach for controller placement problem in large-scale software defined networkings", *Computer Communication*, vol. 112, pp. 24–35, Jan 2017, Available: https://doi.org/10.1016/j.comnet.2016.10.014 (accessed on 15 Dec 2020).

[39] A. Jalili, M. Keshtgari, R. Akbari and R. Javidan, "Multi criteria analysis of controller placement problem in software defined networks", *Computer Communication*, vol. 133, pp. 115–128, Jan 2019, Available: https://doi.org/10.1016/j.comcom.2018.08.003 (accessed on 15 Dec 2020).

[40] B. P. R. Killi and S. V. Rao, "Towards improving resilience of controller placement with minimum backup capacity in software defined networks", *Computer Networks*, vol. 149, pp. 102–114, Feb 2019, Available: https://doi.org/10.1016/j.comnet.2018.11.027 (accessed on 15 Dec 2020).

[41] V. Ahmadi and M. Khorramizadeh, "An adaptive heuristic for multiobjective controller placement in software-defined networks", *Computer & Electrical Engineering*, vol. 66, pp. 204–228, Feb 2018, Available: https://doi.org/10.1016/j.compeleceng.2017.12.043 (accessed on 15 Dec 2020).

[42] 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, June 2020, Available: https://doi.org/10.1109/LCOMM.2020.2979072 (accessed on 15 Dec 2020).

[43] Sood, K. and Xiang, Y., "The controller placement problem or the controller selection problem?", *Journal of Communications and Information Networks*, 2, 1–9, 2017, Available: https://doi.org/10.1007/s41650-017-0030-x (accessed on 15 Dec 2020).

[44] Minzhe Guo and Prabir Bhattacharya, "Controller Placement for Improving Resilience of Software-Defined Networks", *Proceedings of the 2013 Fourth International Conference on Networking and Distributed Computing (ICNDC '13)*, IEEE Computer Society, Washington, DC, USA, pp 23-27, 2013, Available: https://doi.org/10.1109/ICNDC.2013.15 (accessed on 11 June 2018).

[45] H. K. Rath, V. Revoori, S. M. Nadaf and A. Simha, "Optimal controller placement in Software Defined Networks (SDN) using a non-zero-sum game", *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, Sydney, NSW, pp. 1-6. 2014, Available: https://doi.org/10.1109/WoWMoM.2014.6918987 (accessed on 11 June 2018).

[46] P. Xiao, W. Qu, H. Qi, Z. Li and Y. Xu, "The SDN controller placement problem for WAN", *Proceedings of the IEEE/CIC International Conference of Communications in China (ICCC)*, Shanghai, China, pp. 220–224, Oct 2014.

[47] M.R. Haque, S.C. Tan, Z. Yusoff, K. Nisar, C.K. Lee, R. Kaspin, B.S. Chowdhry and R. Buyya, "A New Model for Smart Controller Placement for Uninterrupted SDN Services during Distributed Denial of Service Attacks", *IEEE Access*, November, 2020.

[48] A. Sallahi and M. St-Hilaire, "Optimal Model for the Controller Placement Problem in Software Defined Networks", *IEEE Communications Letters*, vol. 19, no. 1, pp. 30-33, Jan 2015, Available: https://doi.org/10.1109/LCOMM.2014.2371014 (accessed on 13 Feb 2019).

[49] M. F. Bari *et al.*, "Dynamic controller provisioning in software defined networks", *Proceedings of the International Conference of Networks Service Management (CNSM)*, Zürich, Switzerland, pp. 18–25, Oct. 2013.

[50] B. P. R. Killi and S. V. Rao, "Capacitated Next Controller Placement in Software Defined Networks", *IEEE Transactions on Network and Service Management*, vol. 14, no. 3, pp. 514-527, Sept 2017. Available: https://doi.org/10.1109/TNSM.2017.2720699 (accessed on 11 June 2018).

[51] Qi H. and Li K., "Software-Defined Networking Controller Placement in Distributed Datacenters", In: Software Defined Networking Applications in Distributed Datacenters, Springer Briefs in Electrical and Computer Engineering. Springer, Cham, 2016, Available: https://doi.org/10.1007/978-3-319-33135-5_3 (accessed on 11 June 2018).

[52] Dhawan, M., Poddar, R., Mahajan, K., Mann, V., "SPHINX: detecting security attacks in software defined networks", *NDSS*, pp. 1–15, 2015.

[53] 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.

[54] J. Zhang, P. Liu, J. He and Y. Zhang, "A Hadoop Based Analysis and Detection Model for IP Spoofing Typed DDoS Attack", *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, pp. 1976-1983, 2016, Available: https://doi.org/10.1109/TrustCom.2016.0302 (accessed on 13 Mar 2019).

[55] K. D. Joshi and K. Kataoka, "pSMART: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN", *Computer Networks*, ISSN 1389-1286, vol. 178, Art. no. 107295, 2020, Available: https://doi.org/10.1016/j.comnet.2020.107295 (accessed on 13 Mar 2019).

[56] J. Ashraf and S. Latif, "Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques", *2014 National Software Engineering Conference*, Rawalpindi, pp. 55-60, 2014, Available: https://doi.org/10.1109/NSEC.2014.6998241 (accessed on 12 June 2018).

[57] XU Xiaoqiong, YU Hongfang, and YANG Kun, "DDoS Attack in Software Defined Networks: A Survey", *ZTE Communications*, Vol.15 No. 3, P. 13-19, DOI: 10.3969/j.issn.1673⊙5188.2017.03.003, August 2017.

[58] Marius Vochin, Eugen Borcoci and Tudor Ambarus, "On Multi-controller Placement Optimization in Software Defined Networking based WANs", *The Fourteenth International Conference on Networks ICN*, Barcelona, Spain, 2015, Available: https://www.researchgate.net/publication/291274205 (accessed on 13 Nov 2020).

[59] 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", *Lecture Notes in Electrical Engineering*, Springer Nature Singapore Pte Ltd., Springer, Singapore, vol 481, pp 195-203, Print ISBN: 978-981-13-2621-9, Online ISBN: 978-981-13-2622-6, 2019, Available : https://doi.org/10.1007/978-981-13-2622-6_20, (accessed on 6 March 2020).

[60] S. Yang, L. Cui, Z. Chen and W. Xiao, "An Efficient Approach to Robust SDN Controller Placement for Security", *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1669-1682, Sept 2020, Available: https://doi.org/10.1109/TNSM.2020.2994837 (accessed on 13 Nov 2020).

[61] M.R. Haque, S.C. Tan, Z. Yusoff, K. Nisar, C.K. Lee, B.S. Chowdhry, S. Ali, R. Kaspin and S. K. Memona, "SDN Architecture for UAVs and EVs using Satellite: A Hypothetical Model and New Challenges for Future", *CCNC 2021 WKSHPS TCB6GN*, December, 2020.

[62] 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 (JNCA)*, ISSN: 1084-8045, USA, Vol. 36, No. 2, pp. 933-948, March 2013, Available: https://doi.org/10.1016/j.jnca.2012.07.019 (accessed on 13 Mar 2019).

[63] F. Sattar, M. Hussain and K. Nisar, "A secure architecture for open source VoIP solutions", *2011 International Conference on Information and Communication Technologies*, Karachi, pp. 1-6, 2011, Available: https://doi.org/10.1109/ICICT.2011.5983558 (accessed on 13 Sep 2019).

[64] K. Nisar, A. M. Said, and H. Hasbullah, "Enhanced Performance of Packet Transmission Using System Model Over VoIP Network" International Symposium on Information Technology 2010 (ITSim 2010), IEEE 2010, KLCC, Kuala Lumpur, Malaysia, pp. 1005-1008, 15, June 2010, Available: https://doi.org/10.1109/ITSIM.2010.5561593 (accessed on 11 Jan 2020).

[65] S. Chaudhary, A. Amphawan, K. Nisar, "Realization of free space optics with OFDM under atmospheric turbulence", *Optik*, 125, Iss. 18, pp. 5196- 5198, September 2014.

[66] 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*, Taylor & Francis, Vol. 59, No 20, pp. 1745-1752, 28, November 2012. Available: https://doi.org/10.1080/09500340.2012.739713 (accessed on 17 May 2020).

[67] R. Singh and G. Soni, "Realization of OFDM based free space optics", *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, pp. 32-35, 2015.

[68] J. Shuja, R. W. Ahmad, A. Gani, A. I. A. Ahmed, A. Siddiqa, K. Nisar, S. U. Khan, and A. Y. Zomaya, "Greening emerging IT technologies: techniques and practices", *Journal of Internet Services and Applications*, vol. 8, pp 01-11, July 2017, Available: https://doi.org/10.1186/s13174-017-0060-5 (accessed on 13 Sep 2020).

[69] 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*, Association of Computer Electronics and Electrical Engineers, ACEEE, Vol. 10, No. 1, pp. 186-202, January 2014, Available: https://www.scribd.com/document/202469971/A-Distributed-QoS-Oriented-Model-to-Improve-Network-Performance-for-Fixed-WiMAX (accessed on 13 Sep 2020).

[70] I. A. Lawal, A. M. Said, K. Nisar, P. A.Shah, and A. A. Mu'azu, "Throughput Performance Improvement for VoIP Applications in Fixed WiMAX Network Using Client–server Model", *Journal of Science International*, Lahore, ISSN 1013-5316; vol. 26 No. 3, pp 999-1002, August 2014 , Available: http://www.sci-int.com/Search?catid=33 (accessed on Oct 2020).

[71] Y. Maeda, Z. Yan, P. Zhiwei, Yong-Jin, W. Kameyama, K. Nisar, A. A. A Ibrahim, M. H. A. Hijiazi, and H. Kim, "B-6-133 Push-type Content Delivery over 5G Mobile Communication System in NDN", Proceedings of the IEICE General Conference, *The Institute of Electronics, Information and Communication Engineers*, Tokyo, Japan, vol. 2, pp. 133, 2016, Available: https://ci.nii.ac.jp/naid/110010038014/en/ (accessed on Oct 2020).

[72] Z. Yan, G. Geng, H. Nakazato, Y. Park, K. Nisar and A. A. A. Ibrahim, "On-Demand DTN Communications in Heterogeneous Access Networks Based on NDN", *2017 IEEE 85th Vehicular Technology Conference (VTC*

Spring), Sydney, NSW, pp. 1-2, 2017, Available: https://doi.org/10.1109/VTCSpring.2017.8108641 (accessed on Oct 2019).

[73] L. X. Wee, Z.Yan, Y.J. Park, Y. Leau, K. Nisar and A.A. Ibrahim, "ROM-P: Route Optimization Management of Producer Mobility in Information-Centric Networking", *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 267, Springer, Cham, pp 81-91, February 2019 , Available: https://doi.org/10.1007/978-3-030-14757-0_7 (accessed on May 2020).

[74] K. Nisar, I. Welch, R. Hassan, A. Hassan Sodhro, S. Pirbhulal, "A Survey on the Architecture, Application, and Security of Software Defined Networking", *Internet of Things*, 100289, ISSN 2542-6605, 2020,Available: https://doi.org/10.1016/j.iot.2020.100289 (accessed on October 2020).

[75] R. Etengu, S. C. Tan, L. C. Kwang, F. M. Abbou and T. C. Chuah, "AI-Assisted Framework for Green-Routing and Load Balancing in Hybrid Software-Defined Networking: Proposal, Challenges and Future Perspective", *IEEE Access*, vol. 8, pp. 166384-166441, 2020.

[76] M.R. Haque, S.C. Tan, C.K. Lee, Z. Yusoff, S. Ali, R. Kaspin and S. R. Ziri, "Analysis of DDoS Attack-Aware Software-Defined Networking Controller Placement in Malaysia", *Recent Trends in Computer Applications*, Springer International Publishing AG, Springer Nature, Cham, Switzerland, pp 175-188, Print ISBN: 978-3-319-89913-8, Online ISBN: 978-3-319-89914-5, 2018.