*Computers, Materials & Continua*
DOI:10.32604/cmc.2022.018505
***Article***

Tech Science Press

# Unprecedented Smart Algorithm for Uninterrupted SDN Services During DDoS Attack

**Muhammad Reazul Haque[1], Saw Chin Tan[1], Zulfadzli Yusoff[2,*], Kashif Nisar[3,7], Rizaludin Kaspin[4], Iram Haider[3], Sana Nisar[3], J. P. C. Rodrigues[5,6], Bhawani Shankar Chowdhry[7], Muhammad Aslam Uqaili[7], Satya Prasad Majumder[8], Danda B. Rawat[9], Richard Etengu[1] and Rajkumar Buyya[10]**

[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, 63000, Cyberjaya, Selangor, Malaysia
[5]Federal University of Piauí (UFPI), Teresina, PI, Brazil
[6]Instituto de Telecomunicações, 6201-001, Covilhã, Portugal
[7]National Center of Robotics and Automation-Condition Monitoring Systems Lab, MUET, Jamshoro, Pakistan
[8]Department of Electrical and Electronic Engineering, BUET, Dhaka, 1205, Bangladesh
[9]Department of Electrical Engineering and Computer Science, Data Science and Cybersecurity Center, Howard University, Washington, DC, USA
[10]Cloud Computing and Distributed Systems (CLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Melbourne, VIC 3053, Australia
[*]Corresponding Author: Zulfadzli Yusoff. Email: zulfadzli.yusoff@mmu.edu.my
Received: 10 March 2021; Accepted: 02 May 2021

**Abstract:** In the design and planning of next-generation Internet of Things (IoT), telecommunication, and satellite communication systems, controller placement is crucial in software-defined networking (SDN). The programmability of the SDN controller is sophisticated for the centralized control system of the entire network. Nevertheless, it creates a significant loophole for the manifestation of a distributed denial of service (DDoS) attack straightforwardly. Furthermore, recently a Distributed Reflected Denial of Service (DRDoS) attack, an unusual DDoS attack, has been detected. However, minimal deliberation has given to this forthcoming single point of SDN infrastructure failure problem. Moreover, recently the high frequencies of DDoS attacks have increased dramatically. In this paper, a smart algorithm for planning SDN smart backup controllers under DDoS attack scenarios has proposed. Our proposed smart algorithm can recommend single or multiple smart backup controllers in the event of DDoS occurrence. The obtained simulated results demonstrate that the validation of the proposed algorithm and the performance analysis achieved 99.99% accuracy in placing the smart backup controller under DDoS attacks within 0.125 to 46508.7 s in SDN.

**Keywords:** SDN; smart algorithm; RTZLK-DAASCP; DDoS attack; DRDoS

## 1 Introduction

Software-defined networking (SDN) has attained evident quality worldwide since it is agile, programmable [1], cost-effective, besides the centralized networking system framework in contrast with the customary traditional computer, telecommunications, and satellite communication frameworks that are more confounded and harder to oversee. The focal point of SDN engineering is the controller that mediates among clients and assets to deliver services [2–4]. SDN enables industry operators to reduce operational expenditure (OPEX) and capital expenditure (CAPEX) and create innovative, differentiated services [5]. SDN's principal function is to expedite and progress the network management system with high flexibility and reliability by separating the control plane from the data plane. Moreover, the capability to unlock more innovative opportunities is owed to the network programmability of SDN. Numerous researchers from both industrial and academic have been attracted to address SDN issues [6]. Open Networking Foundation (ONF) states that SDN is a developing design that is dynamic, reasonable, financially savvy, and versatile, making it ideal for the high-bandwidth, dynamic nature of emerging applications [7]. Before SDN was engineered, the goal to make a programmable networking system had for long been thought of by researcher; for instance, the scientists in [8–14] upheld fast programmable data handling.

The brain of SDN is the controller, which comprises many uses giving united control usefulness through an open application program interface (API) to process the network data packet through an open interface. The SDN controller is a coherent control structure that runs the Network Operation System (NOS) [15]. The equipment deliberations to the control plane, which can monitor the global view of the network architecture. The kernel brainchild of SDN is to separate the control plane and the data plane [16,17] by creating a particular software that allows the operating system of the network (software controller) of SDN to operate on separate hardware (physical controller) [18]. Fig. 1 shows a typical architecture of SDN.

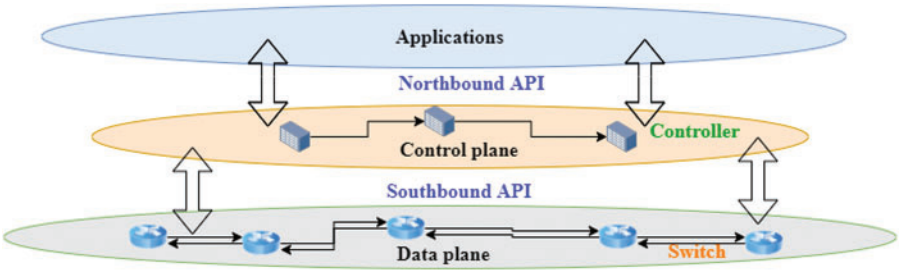


**Figure 1:** Simplified architecture of SDN [19]

This separation not only provides a significant feature for future networks and telecommunication but also threatens SDN security. SDN is a structure designed to simplify and improve network management with high flexibility by splitting the control plane and data plane [20].

Distributed denial of services (DDoS) attack attempts to make an online service or network unavailable by creating excessive requests from the OpenFlow switch to the controller. The various attack sources include all personal computers (PC), servers, smartphones, alarm systems, cameras, the Internet of things (IoT) devices, and sensors. DDoS attacks can paralyze SDN services by overwhelming servers, network links, and network devices (routers, switches, and controllers.) with illegitimate traffic. They can either cause service degradation or complete denial of service, causing huge losses [21]. In Fig. 2, we give an illustration of how the DDoS attack operated in general.


**Figure 2:** DDoS attack on SDN controller

Initially, attackers will infiltrate the controller via either a PC, smartphone, and IoT sensor. Through switches by using a botnet or a zombie. As a result, all the devices connected to the victim controller will eventually malfunction. Moreover, an infrastructure layer (switch) will typically request the controller to obtain new rules when it cannot handle data packets or forward data packets due to a mismatch in the flow table [22]. Also, a large volume of DDoS attack traffic would occupy the entire bandwidth [23], causing congestion that would result in the controller becoming slow. Eventually, malfunction will occur after encountering DDoS attacks continuously. If the controller becomes the victim of a DDoS attack, all the switches connected to that controller will have malfunctioned and unable to serve the legitimate users. Hence, it is necessary to install an alternative controller to serve legitimate users.

The controller is the most critical component in the SDN network. Hence, controller placement in SDN planning is one of the critical criteria for providing uninterrupted services. Lately, it accounted for intimidation based on Distributed Denial of Service (DDoS) or Ransom Denial of Service (RDoS), an attacker professing to attack 'Lazarus'. The attacker was threatening to dispatch a DDoS attack against the customer's entire organization if the owner does not pay the installment within six days. DDoS attacks do not generally accompany a payment interest, yet, given that even one hour of downtime can cost organizations up to $100K sometimes, this sort of RDoS attacks merits viewing appropriately and relieving against services. The highest attacking data packet was 700 GigaByte Per Second (Gbps) or 6,012,951,135,769 bits per second, depicted in Fig. 3 [24].

In the first few weeks of January 2021, DRDoS and RDoS attacks on German organizations and government offices have gotten increasingly continuous. Cybercriminals are utilizing the force of volumetric reflection attacks to coerce enormous ransoms. A Distributed Reflected Denial of Service (DRDoS) attack is an exceptional type of DDoS. For this situation, malevolent solicitations do not start from the actual attacker or a botnet setup. However, from specific Internet services [25], So DRDoS attack is an upcoming strong threat for SDN controllers with DDoS attack. Assurance for SDN networks is winding up being logically more essential in the field of security. This condition is being experienced despite that SDN can give a rich network. In any case, SDN faces different security challenges [26], simultaneously, for example, DDoS attack, network hindering, switch information spillage, management classification, and different principle

attacks in traditional networks [27]. From this time forward, it is imperative to pass on various reinforcement controllers to give non-stop SDN services under different DDoS attacks. Here, we proposed a smart algorithm to estimate the numbers of backup controllers required to be deployed at any specific location or node where DDoS occurred.

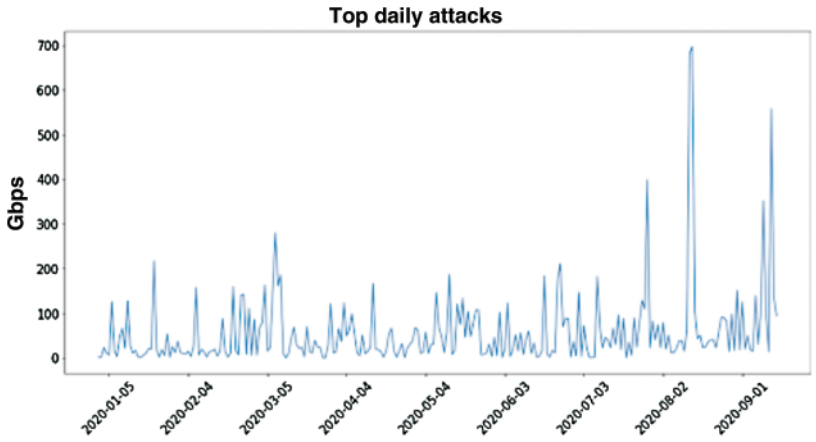


**Figure 3:** Gbps of DDoS attacks per day as observed in 2020

We organized this paper as follows. In the next section, we presented related work and the development of our proposed backup controller placement smart algorithm, Reazul Tan Zul Lee Kashif (called RTZLK) DDoS Attack Aware SDN Smart Controller Placement Algorithm (called DAASCPA). The flowchart of the proposed algorithm is disclosed in Section 3. Evaluation of the proposed smart algorithm under various scenarios will be conducted, and the result of the layout plan diagrams is shown in Section 4. A vision and future directions are discussed in Section 5. Finally, a conclusion is drawn in Section 6.

## 2 Related Work

First, the authors in [28] proposed the SDN controller placement by utilizing the k-median, comparing the advancement issue heuristic algorithm and the k-center, and the related improvement issue heuristic algorithm. Their work centered around the controller's latency, the controller's reaction time and did not address the controller placement under DDoS attack. In [29], the authors raised a standard system to change the connection between the controller and the switches dependent on the conduct of the controller position issue. The authors in [30] considered the need to augment the unwavering quality of the SDN controllers utilizing heuristic algorithms and brute force. In [31], the authors considered the controller placement issue was decreasing the most noticeably awful dormancy of the control ways under satisfying the heap limitation of SDN controllers. In [32], without referencing the DDoS attack, the author presented another upgraded model for the SDN controller placement just as switches and connections in the SDN. The authors in [33] focused on the need to delineate the weakness of SDN to DDoS attacks in cloud computing. They researched the new inclination and highlight of DDoS attacks in the cloud computing environment and gave a comprehensive measure of walled-in area systems against DDoS attacks utilizing SDN. In [34], the authors presented a DDoS attack safeguard by DDoS hindering framework by utilizing OpenFlow interface. In light of expeditiousness, flexibility, and exactness, the authors proposed a DDoS attack discovery technique in [35].

The authors in [36] proposed a multi-line SDN controller planning algorithm dependent on the time cut assignment procedure identified with controller placement in SDN. Based on attack traffic, attack scale, and courses of events, the work in [37] addressed the location of DDoS attacks in cloud services. Nevertheless, their proposed algorithm is a simple link to identify attacks that made the controllers break down, which brought about the interferences of services. In [38], the authors presented pSMART, a lightweight, security-mindful assistance work chain orchestration in a multi-space NFV/SDN circumstance, which cannot uphold during the colossal volume of DDoS attack traffic. In [39], the authors' proposed algorithms for exact and heuristic assessments of the resulting and completed in the Matlab-based POCO framework for the Pareto-based Optimal Controller placement. At this point, it does not fulfill the need to offer help during DDoS. The authors in [40] proposed a multi-target ILP definition introduced to derive the related controller position. However, security dangers like DDoS attacks are not considered to offer constant types of assistance. In [41], the authors built up a Parameter Optimization Model (POM) for the heuristic figuring applied to the CPP. The heuristic algorithm can sufficiently disentangle the CPP by using the high-level limits procured in POM. The work does not consider components for securing the SDN controller and framework. In [42], the authors proposed a hypothetical idea of smart controller placement for SDN engineering. Essentially, SDN is poised to apply future applications, for example, voice over IP (VoIP) [43–45], fiber optic [46–48], worldwide interoperability for microwave access (WiMAX) [49–51], and artificial intelligence (AI) and machine learning (ML) [52], deep learning (DL) [53] unmanned aerial vehicle (UAV) and autonomous electric vehicle (AEV) through satellite [54]. The above works neither considered intelligent reinforcement controller algorithm nor DDoS attack danger. In this paper, we proposed a smart algorithm for planning the deployment of SDN controllers under DDoS attack situations, which comprises additional backup reinforcement controllers notwithstanding the current controllers to guarantee the support of real clients without interruption.

## 3 SDN RTZLK-DAASCP Algorithm

Here, we present a DDoS attack-aware smart controller placement algorithm that comprises additional savvy reinforcement controllers notwithstanding the current controllers to guarantee the services for genuine clients without interruption.

### *3.1 Input:*

*R is the number of types of switches in set* $\boldsymbol{S}$, *Set of the switch* $\boldsymbol{S} = \{\boldsymbol{s1}, \boldsymbol{s2}, \boldsymbol{s3} \ldots \boldsymbol{sR}\}$ , $\boldsymbol{Avl^S}$ *is the available data packet in each switch that needs to be processed by the controller,* $\boldsymbol{k}$ *is the number of types of the controllers in set C, Set of controller* $\boldsymbol{C} = \{\boldsymbol{c1}, \boldsymbol{c2}, \boldsymbol{c3} \ldots \boldsymbol{ck}\}$, *Available controller in set* $\boldsymbol{C = c1 = 2, c2 = 1, c3 = 3}$, $\boldsymbol{Prp^C}$ *is the processing power of the controller* $\boldsymbol{C = c1, c2, c3, \ldots ck}$, $\boldsymbol{Port^C}$ *is the port of the controller,* $\boldsymbol{Co^C}$ *is the cost of the controller,* $\boldsymbol{Avl^C}$ *is the availability of the Controller,* $\boldsymbol{m}$ *is the number of types of the backup controller, Set of the smart backup controller* $\boldsymbol{BC} = \{\boldsymbol{bc1}, \boldsymbol{bc2}, \boldsymbol{bc3} \ldots \boldsymbol{bm}\}$ , $\boldsymbol{Prp^{bc}}$ *is the processing power of the backup controller,* $\boldsymbol{Port^{bc}}$ *is the Port of the backup controller,* $\boldsymbol{Co^{bc}}$ *is the cost of the smart backup controller,* $\boldsymbol{Avl^{bc}}$ *is the availability of the smart backup controller,* $\boldsymbol{w}$ *is the number of the nodes,* $\boldsymbol{n = \{n1, n2\ n3, \ldots nw\}}$ *is the node to place controller and smart backup controller, Distance between nodes to place controller* $= \boldsymbol{200\ m}$ , $\boldsymbol{DDoS^n}$ *is the DDoS attack on node* $n$, $\boldsymbol{Aff^c}$ = *affected controller in* $\boldsymbol{C = \{c1, c3\}}$, *and* $\boldsymbol{Aff^n}$ = *affected node in* $\boldsymbol{n = \{n1, n3\}}$.

### 3.2 Output:

*The controller and the smart backup controller placement matrix* $T^{c}n$ , $T^{BC}n$.

### 3.3 Algorithm:

*1:* ***Start***

***Initialization:***

*The controller placement matrix* $T^{c}n$ *to* **0** *for controller type c at all node n,* **cp** *= The controller placement, temporary controller placement list* $T^{cp}list = 0$, *Smart backup controller placement matrix* $T^{BC}n$ *to* **0** *for the smart backup controller type* **b** *at all node* **n**, **bcp** *= The smart backup controller placement, Temporary smart backup controller placement list* $T^{bcp}list = 0$, $Avl^{S}$ **=** *The available data packet in the switch that needs to be processed by the controller,* $Co^{c}Min$ *= The minimum cost of the controllers,* $Co^{b}Min$ *= The minimum cost of the smart backup controllers,* **cs** *= Controller's subset,* $SPP^{cs}$ *= The sum of the processing power of the controller's Subset,* $SPort^{CS}$ **=** *The sum of port of the controller's subset,* $SCo^{CS}$ *=The sum of the cost of the controller's subset,* $SCo^{CS}Min$ *= The minimum cost of the controller's subset,* $Req^{n}$ *= The number of the required node,* **P** *= Power set* **z[P(C)]** *= The number of element (controller) in Power Set.*

*2:* ***foreach*** *items in the controller's set* $C = \{c1, c2, c3 \ldots, ck\}$

*3:* ***Create*** *a* ***Union of set*** *with available controllers of each type of the controller from* ***Set C***

***c1*** ∪ ***c2*** ∪ ***c3*** …∪ ***ck*** **=** {*c1 [1], c1 [2], c2 [1], c3 [1], c3 [2], c3 [3]…,ck[k]*}

*4:* ***Update*** *it in set* **C** = {*c1 [1], c1 [2], c2 [1], c3 [1], c3 [2], c3 [3]…,ck*}

*5:* ***Create a Power Set P(C)*** *for the set of the* ***Controller*** $C = \{c1[1], c1[2], c2[1], c3[1], c3[2], c3[3] \ldots, ck\}$

*For set* $C = \{c1[1], c1[2], c2[1], c3[1], c3[2], c3[3] \ldots, ck\}$ *calculate the following subsets*

*Subsets with 0 controller*−{∅}{∅} *(the empty set)*

*Subsets with 1 controller*− $\{c1[1]\}, \{c1[2]\}, \{c2[1]\}, \{c3[1]\}, \{c3[2]\}, \{c3[3]\} \ldots \{ck[k]\}$

*Subsets with 2 controllers–*

{*c*1[1], *c*1[2]},*c*1[1], *c*2[1], *c*1[1], *c*3[1]}, {*c*1[1], *c*3[2]}, {*c*1[1], *c*3[3]}, {*c*1[1], *ck*[*k*]}, {*c*1[2], *c*2[1]}, {*c*1[2], *c*3[1]}, {*c*1[2], *e*}, {*c*1[2], *c*3[3]}, {*c*1[2], *ck*[*k*]}, {*c*2[1], *c*3[1]}, {*c*2[1], *c*3[2]}, {*c*2[1], *c*3[3]}, {*c*2[1], *ck*[*k*]}, {*c*3[1], *c*3[2]}, {*c*3[1], *c*3[3]}, {*c*3[1], *ck*[*k*]}, {*c*3[2], *c*3[3]}, {*c*3[2], *ck*[*k*]}, {*c*3[3], *ck*[*k*]}

*Subsets with k controllers*−{*c*1[1], *c*1[2], *c*2[1], *c*3[1], *c*3[2], *c*3[3] … *ck*}

*6:* ***Compute*** *the sum of the* ***processing power*** *of the elements (controllers) in each subset* $SPP^{cs}$ *from* ***Power Set*** *z[P(C)] and* ***update*** *it in the temporary controller placement list* $T^{cp}list$

*7:* $T^{cp}list \leftarrow SPP^{cs}$.

*8:* ***Compute*** *the sum of the* ***port*** *of the elements (controllers) in each subset* $SPort^{CS}$ *from* ***Power Set*** *z[P(C)] and* ***update*** *it in the temporary controller placement list* $T^{cp}list$

*9:* $T^{cp}list \leftarrow SPort^{cs}$.

*10:* ***Compute*** *the sum of the* ***cost*** *of the elements (controllers) in each subset* $SCo^{cs}$ *from* ***Power Set*** *z[P(C)] and* ***update*** *it in the temporary controller placement list* $T^{cp}list$

*11:* $T^{cp}list \leftarrow SCo^{cs}$.

*12:* ***Compute*** *the Sum of* $\sum Avl^{S}$ *from the set* $S = \{s1, s2, s3 \ldots sR\}$

13: **Calculate** the Required Processing power of the subset $Prp^{CS} = \sum Avl^{S}$
14: **Calculate** the Required $Port^{C}$ = The number of the switches in set $S = \{s1, s2, s3 \ldots sR\}$
15: **for** $(i = 0; i \geq ck; i{+}{+})$
{
16: **iff** $Avl^{C} \neq 0$, **go to step 16**
17: **else Stop:** The controller is not available
18. **if** Subset_ $Prp^{CS} < \sum Avl^{S}$
19: **Stop:** The controller does not exist with the required processing power
20: **else** go to next step
21: **if** $Port^{CS} <$ Required $Port^{C}$
22: **Stop:** The controller does not exist with the required port
23: **else** go to step 24
{
24: **for** $(j = 0; j \geq z[P(C)]; j{+}{+})$
25: **for each** items in $\boldsymbol{T^{cp}}$**list**
26: **if** $Prp^{CS} \geq \sum Avl^{S}$
27: &&$Port^{CS} \geq$ Required $Port^{C}$
28: **update** the subset_of_Controller [i] in $\boldsymbol{T^{cp}}$**list**
**end iff**
**end else**
**end if**
**end else**
**end if**
**end else**
**end for**
**end foreach**
**end if**
}
29: **Update** the controller subset with the minimum cost from $\boldsymbol{T^{cp}}$**list** $\leftarrow$ $\boldsymbol{SCo_{\_}^{CS}}$ **Min**
30: **NoOfchosenController == Updated** $\boldsymbol{T^{cp}}$**list**
31: Number of Required Node, $\boldsymbol{Req^{n}}$ == NoOfchosenController
32: **Select** the$\boldsymbol{Req^{n}}$ from n = n1, n2 n3 . . .nW
33: $\boldsymbol{Req^{n}} \leftarrow n$
34: place the controller on the selected node
35: $\boldsymbol{T^{c}n} \leftarrow$ **Updated** $\boldsymbol{T^{cp}}$**list**
36: **Display** $\boldsymbol{T^{c}n}$

```
            }
37          : for (y = 0; y ≥ nw; y++)
            {
38: if DDoS^N ≠ 0
39: The required processing power of the smart backup Controller Prp^bc = processing power of Aff^c
40: Required Port^bc = Port of Aff^c
            {
41:         for (z = 0; z ≥ bm; z++)
42: iff Avl^bc ≠ 0, go to step 40
        else Stop: The Smart backup controller is not available
43: if Prp^bc < Processing Power of Aff^c
44:             Stop: The smart backup controller does not exist with the required processing power
45:       else go to next step
46:           if Port^bc < Port of Aff^c
47:             Stop: The smart backup controller does not exist with the required port
48:       else go to next step
49:           foreach items in BC = {b1, b2, b3 . . . bm}
50:             if Prp^bc ≥ Aff^c
51:                 && Port^bc ≥ Port of Aff^c
52:                 && cost of the smart backup controller == Co_bc Min
53:       Place it on Aff^n
54:           Display T^bc n
                    end iff
                  end else
                end if
                end else
              end if
          end else
                end foreach
                  end if
            }
              }
                else
                  exit
                    end if
55: Stop
```

### *3.4 Flowchart of The Algorithm*

We illustrated the flowchart of the RTZLK-DAASCP algorithm in Fig. 4.

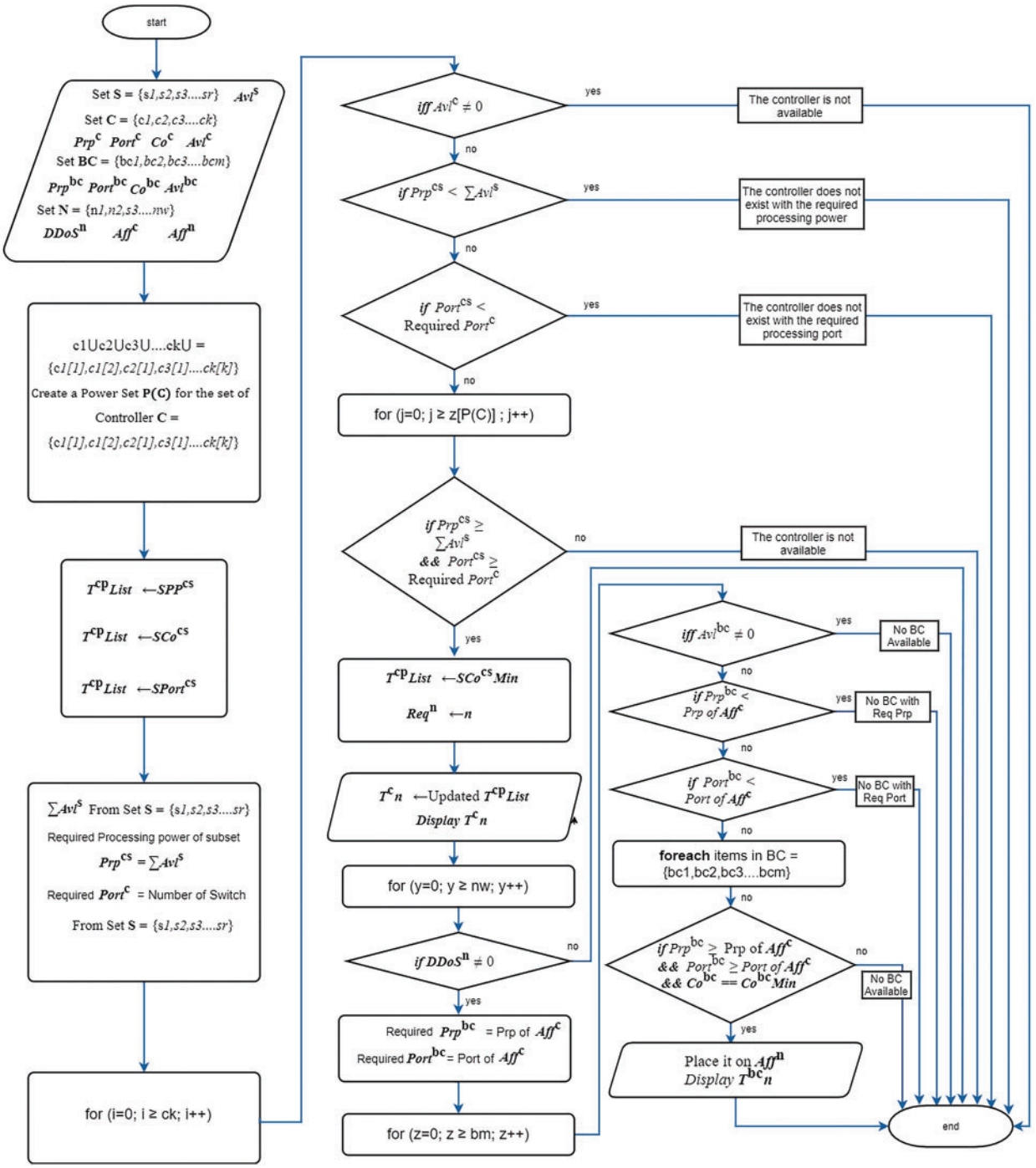


**Figure 4:** Flowchart of RTZLK-DAASCP algorithm

## 4 Result and Diagrams

Our proposed algorithm has been developed using A Mathematical Programming Language (AMPL) [55], which supports formulation, testing & deployment, and IBM ILOG CPLEX [56] with Intel (R) Core (TM) i7–6700 CPU@3.40 GHz, RAM 8 GB, and virtual memory 128 GB machine. The proposed smart algorithm is evaluated in several different scenarios. The obtained data from the result presented in Tabs. 1–4. The diagrams from the results show the connection between the controller and a smart backup controller, controllers to controllers, DDoS attacks, and controllers to switches under four typical practical networks given in Figs. 5–8.

**Table 1:** Four SDN controllers placement with 9 switches without DDoS attack

| Number of controllers | Four C3 |
|---|---|
| Processing power | 8000 packets/s (pps) |
| Port | 64 |
| Cost | $4500/C3 Controller |
| Number of switches | 9 |
| Available data packets | 28,840 |
| Link | Link1 |
| Bandwidth | 10000000 Mbps |
| Cost | $0.25/m |
| Frequency of DDoS attack | No |
| Backup controller | No |

**Table 2:** Two SDN controllers placed with 3 switches with 1 backup controller under DDoS attack

| Number of controllers | Two (C1 and C3) |
|---|---|
| Processing power | 8000 packets/s |
| Port | 64 |
| Cost | $4500/Controller |
| Number of switches | 9 |
| Available data packets | 8,800 |
| Link | Link1 |
| Bandwidth | 10000000 Mbps |
| Cost | $0.25/m |
| Frequency of DDoS attack | 1 attack on node 8 |
| Backup controller | BC1 |

The entirety of the over four DDoS attack situations demonstrated that our smart algorithm could guarantee the SDN operation is uninterrupted even under the different frequency of DDoS attack by placing the extra smart backup controller in addition to the existing SDN controller.

**Table 3:** Eight SDN controllers placement with 13 switches and 1 backup controller under DDoS attack

| Number of controllers | One C3, Two C6, Four C9 and One C13 |
|---|---|
| Processing power | 8000, 13000, 13000 and 13000 pps, |
| Port | 64, 128, 128 and 128 |
| Cost | $4500, $9500, $9500 and $9500 |
| Number of switches | 13 |
| Available data packets | 71,900 |
| Link | Link1 |
| Bandwidth | 10000000 Mbps |
| Cost | $0.25/m |
| Frequency of DDoS attack | 1 attack on node 1 |
| Backup controller | BC1 |

**Table 4:** Five SDN controllers placement with 9 switches and 7 backup controllers under DDoS attack

| Number of controllers | One C3, Two C6 and Two C9 |
|---|---|
| Processing power | 8000, 13000 and 13000 pps |
| Port | 64, 128 and 128 |
| Cost | $4500 (C3), $9500 (C6) and $9500 (C9) |
| Number of switches | 9 |
| Available data packets | 49,900 |
| Link | Link1 |
| Bandwidth | 10000000 Mbps |
| Cost | $0.25/m |
| Frequencies of DDoS attack | 1 attack on node 1, 3 attacks on node 2, 2 attacks on node 4 and 1 attack on node 6 |
| Backup controller | 3 BC2, 1 BC3, 1 BC4 and 2 BC5 |

The vital cost concerning repeat of attacks plotted as exhibited in Fig. 9. The cost is going from USD 30,000 for no attack to around USD 50,000 for the triple attack. It will in general be contemplated that insignificant exertion for the low attack, the medium cost is typical for a medium attack and higher cost for the higher attack. Compare to the recently proposed Lightweight algorithm [57] and boosting algorithm [58], The results obtained show that our proposed RTZLK-DAASCP smart algorithm provides uninterrupted SDN services against DDoS attacks with high accuracy and minimum cost.

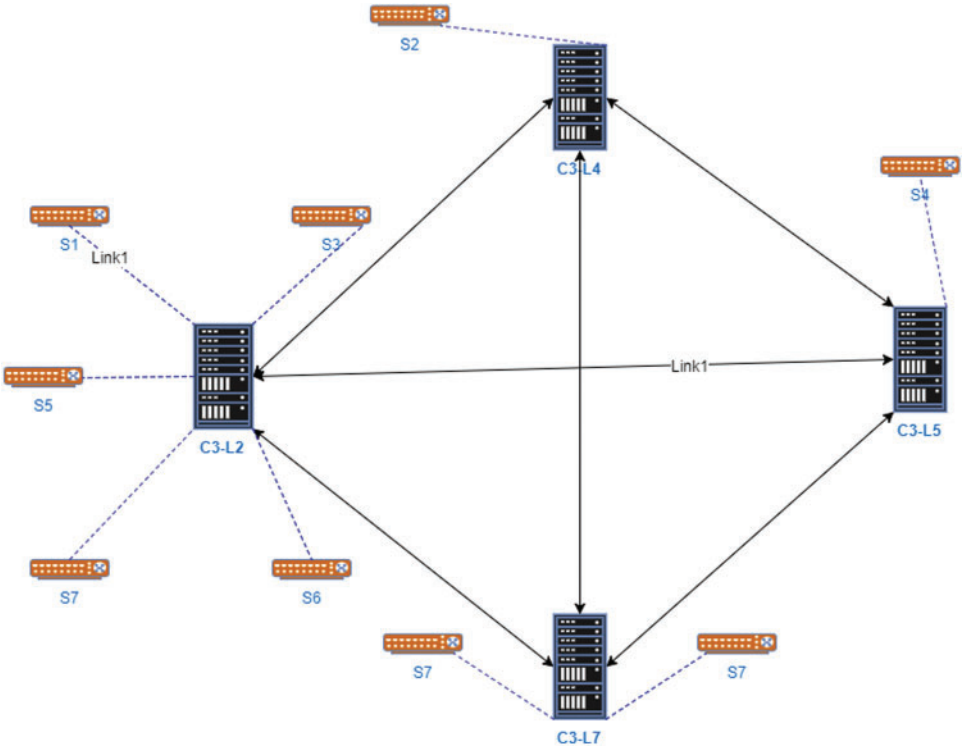


**Figure 5:** Diagram from the result data of Tab. 1

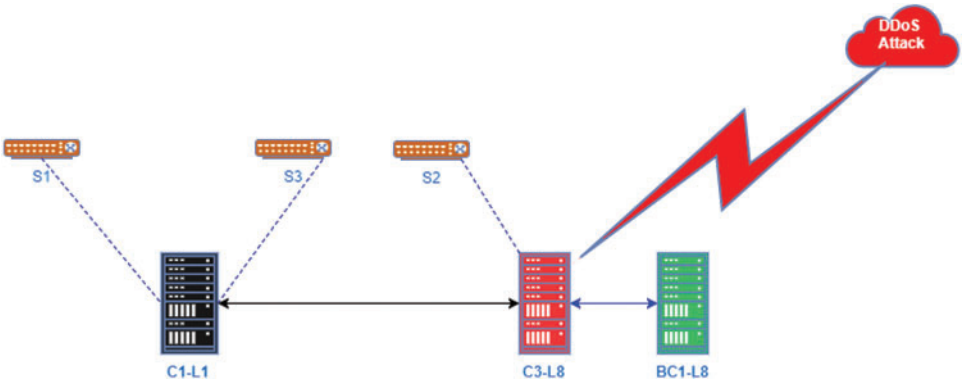


**Figure 6:** Diagram from the result data of Tab. 2

## 5 Vision and Future Directions

The impact of the design and planning of SDN infrastructure varies from different geo-locations. It is necessary to implement the proposed algorithm in real heterogeneous network topologies based on heterogeneous geo-locations.

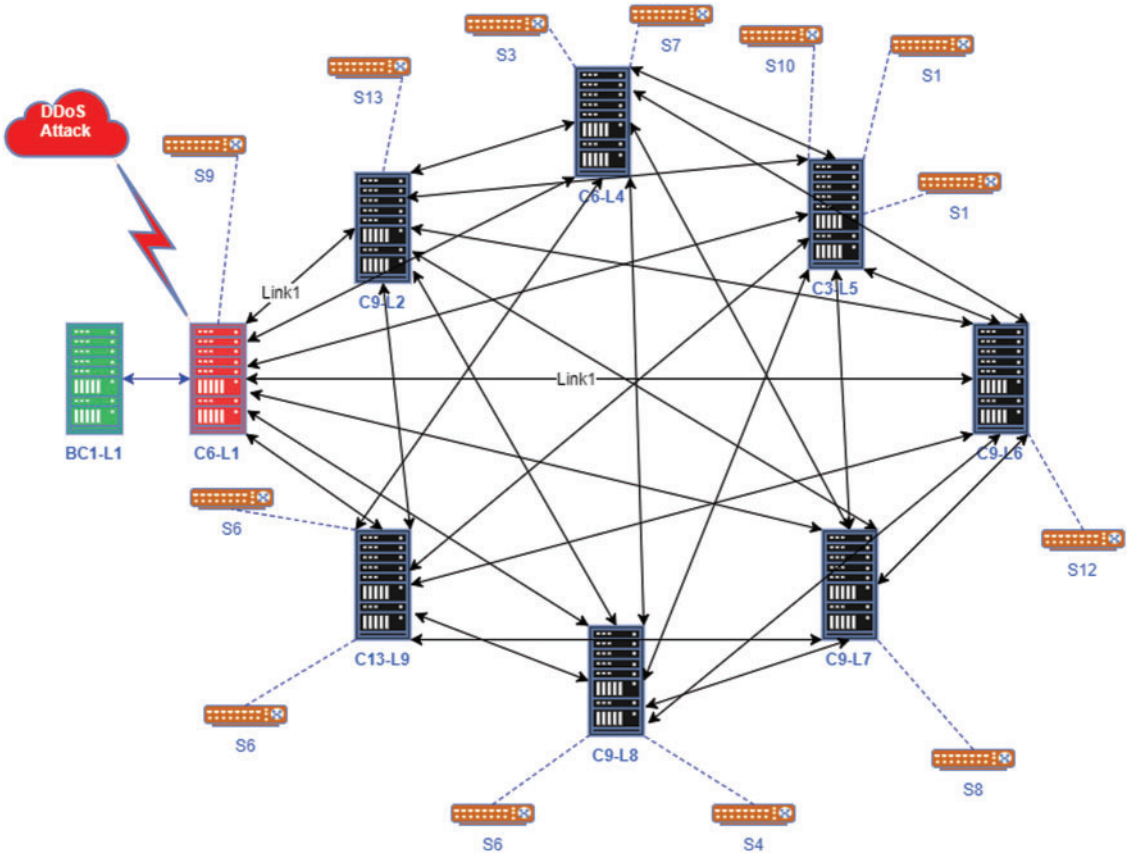


**Figure 7:** Diagram from the result data of Tab. 3

### *5.1 Vision*

IoT devices and sensors, computers, ISPs, telecommunication, satellite communication, and datacenter networking system need SDN to empower dynamic provisioning, advanced network usage, and the making of new wellsprings of income.

### *5.2 Future Direction*

In SDN deployment, there are additional challenges that we should address. One such challenge is that many ISP, Telecommunication or satellite communication operators or equipment manufacturers will require extra preparation, training and activities instruments to exploit SDN, and at last streamline their tasks and the SDN control plane must have the option to help multi-area, multi-layer asset portion and advancement. Our proposed model is suitable for planning and deployment in a real-world networking topology for these two Geo locations: IBM (USA) and KREONET (South Korea) [59]. We are furnishing diagram and real-time dataset [60] from the Internet Topology Zoo and converted using yEd [61], a powerful diagramming program, depicted in Figs. 10 and 11.

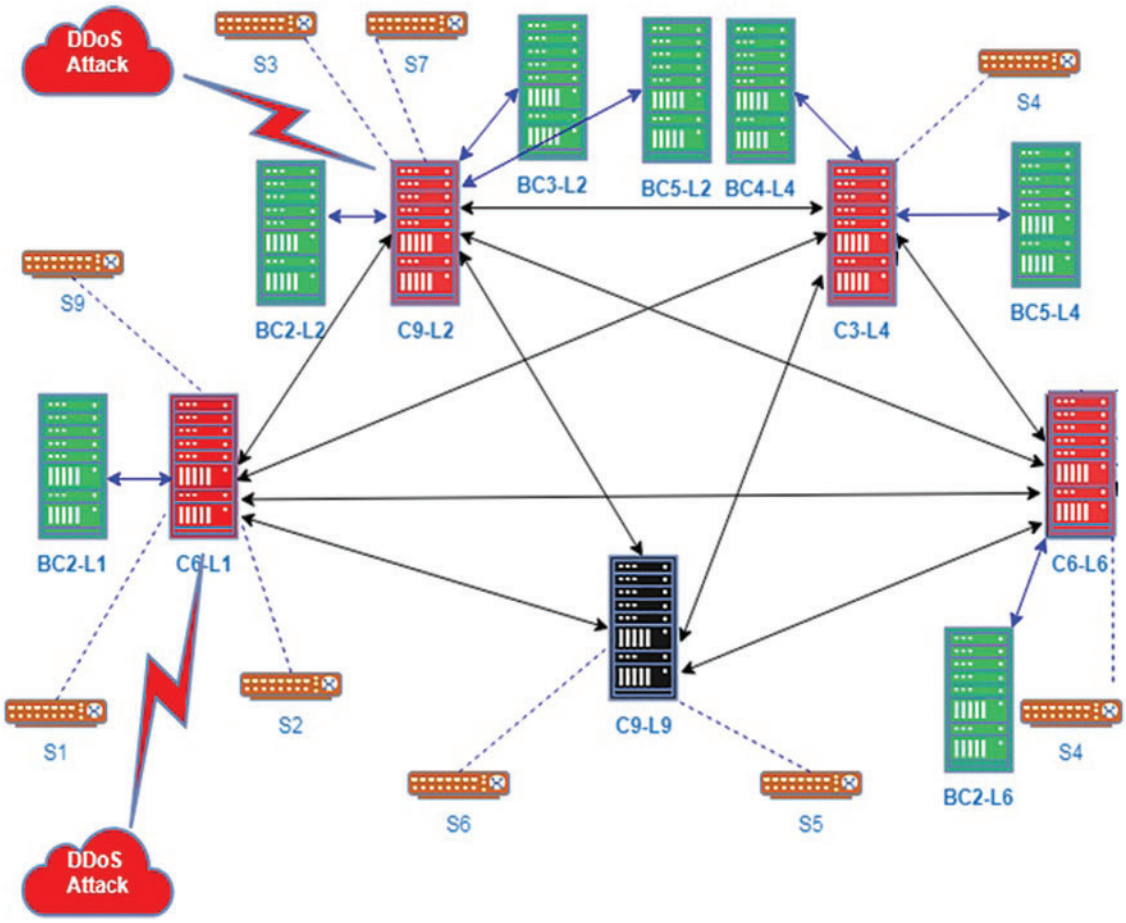


**Figure 8:** Diagram from the result data of Tab. 4

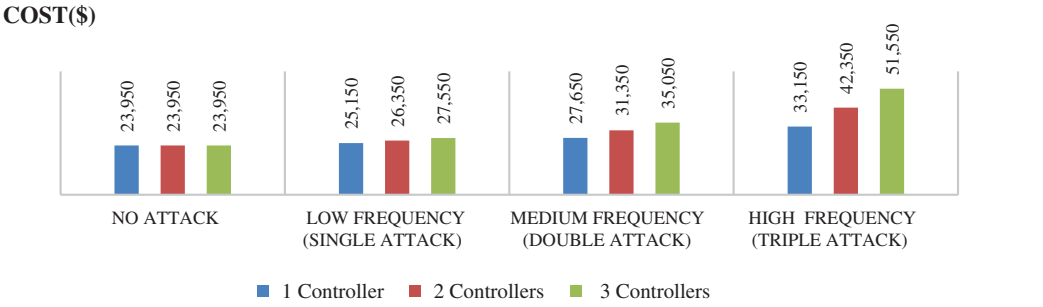


**Figure 9:** The total expense for single or multiple smart backup controllers placements

*5.2.1 Geo Location: IBM (USA)*

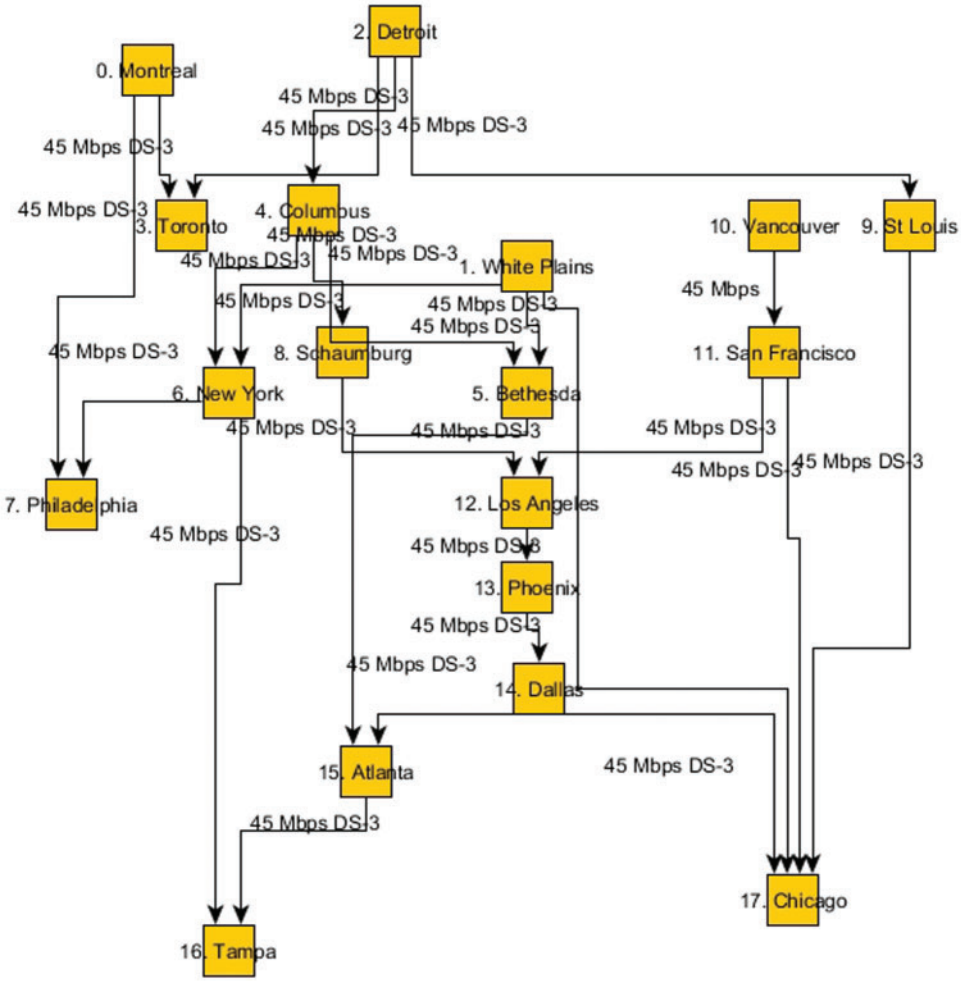


**Figure 10:** The real topology diagram of IBM (USA), data executed by using yEd

*5.2.2 Geo Location: KREONET (South Korea)*

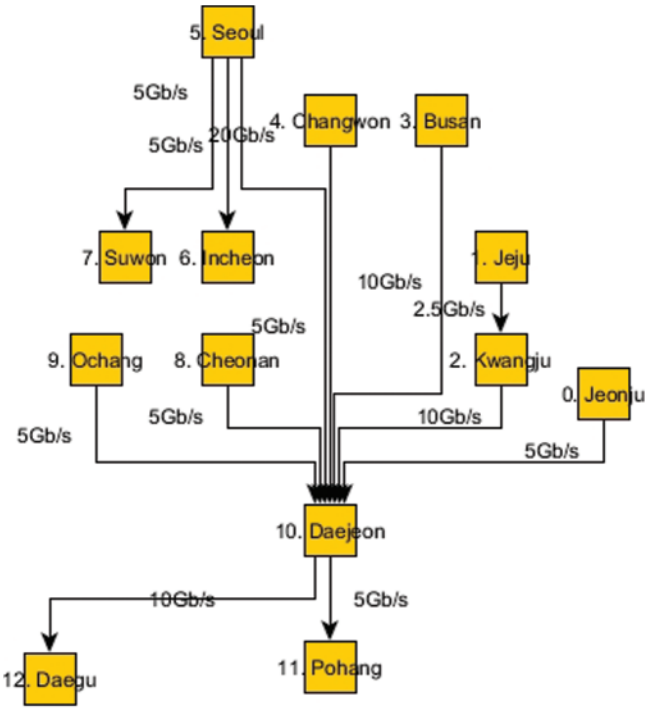


**Figure 11:** The real topology diagram of KREONET (South Korea), data converted by using yEd

## 6 Conclusions and Future Work

The outcomes got from our proposed RTZLK-DAASCP smart algorithm display that we have accomplished the target of limiting complete expense by advancing the necessity of numerous backup controllers dependent on hypothetical frequencies of DDoS attack. The obtained results show that one smart backup controller is installed at a specific location if a solitary attack happens in SDN. A few smart backup controllers will place if SDN experienced twofold or triple attacks. The discoveries exhibited that the proposed smart controller is lithe to confront DDoS attacks by placing a smart backup controller at fitting hubs to guarantee that authentic SDN clients stay continuous. The principle multifaceted nature of the smart algorithm is that it will require more time to plan and design any large-scale SDN. We will stretch out the proposed smart algorithm to deployment of Next Generation SDN (NG-SDN) Infrastructure in future work. We will develop RTZLK-DAA smart controller using DevOps and Mendix via IBM cloud access to the most advanced Quantum Computers and Google Quantum AI to resist DRDoS types of attack. This new research will be a milestone for future design and planning of IoT, telecommunication, and satellite communication systems using SDN.

**Acknowledgement:** The authors would like to thank the editors of CMC and anonymous reviewers for their time and review of this manuscript and Professor Dr. Yong-Jin Park (IEEE Life member and former Director IEEE Region 10) valuable comments and suggestions on improving the paper.

**Funding Statement:** TM R&D Sdn Bhd fully supports this research work under Project RDTC160902. S. C. Tan and Z. Yusoff received the fund. Sponsors' Website: https://www.tmrnd.com.my.

**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] 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.

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson *et al.,* "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review Archive*, vol. 38, no. 2, pp. 69–74, 2008.

[6] 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.

[7] Open Networking Foundation (ONF), "ONF SDN Projects," 2020. [Online]. Available: https://opennetworking.org/onf-sdn-projects/.

[8] 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 *2017 IFIP/IEEE Symp. on Integrated Network and Service Management*, Lisbon, pp. 608–611, 2017.

[9] 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.

[10] 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.

[11] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, C. K. Lee *et al.,* "Automated controller placement for software-defined networks to resist DDoS attacks," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 3147–3165, 2021.

[12] 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.

[13] 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. 195–206, 2010.

[14] K. Nisar, E. R. Jimson, M. Hijazi and K. S., "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.

[15] S. Dong and M. Sarem, "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020.

[16] P. Xia, L. Zhi-yang, G. Song, Q. Heng and Q. Wen-yu, "A Kself-adaptive SDN controller placement for wide area networks," in *Frontiers of Information Technology & Electronic Engineering*, vol. 17. Chinese Academy of Engineering (CAE), Springer & Zhejiang University Press, pp. 620–633, 2016.
[17] 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.
[18] M. Seliuchenko, O. Lavriv, O. Panchenko and V. Pashkevych, "Enhanced multi-commodity flow model for QoS-aware routing in SDN," in *Int. Conf. Radio Electronics & Info Communications*, Kiev, pp. 1–3, 2016.
[19] 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.
[20] G. Wang, Y. Zhao, J. Huang and W. Wang, "The controller placement problem in software defined networking: A survey," *IEEE Network*, vol. 31, no. 5, pp. 21–27, 2017.
[21] R. Masoudi and Ali Ghaffari, "Software defined networks: A survey," *Journal of Network and Computer Applications*, vol. 67, no. 4, pp. 1–25, 2016.
[22] 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.
[23] N. Z. Bawany, J. A. Shamsi and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Arab Journal of Science and Engineering*, vol. 42, no. 2, pp. 425–441, 2017.
[24] 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/.
[25] T. Landscape, *DRDoS & RDoS: Blackmail Using Reflection Attacks*. Germany: Myra Security GmbH, pp. 1, 2021. [Online]. Available at: https://www.myrasecurity.com/en/drdos-rdos-blackmail-using-reflection-attacks.
[26] 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.
[27] 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.
[28] B. Heller, R. Sherwood and N. McKeown, "The controller placement problem," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 473–478, 2012.
[29] 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, pp. 18–25, 2013.
[30] 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," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, no. 5, pp. 92–97, 2012.
[31] 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.
[32] 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.
[33] 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.
[34] S. Lim, J. Ha, H. Kim, Y. Kim and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," in *Sixth Int. Conf. on Ubiquitous and Future Networks*, Shanghai, pp. 63–68, 2014.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] M. R. Haque, S. C. Tan, Z. Yusoff, C. K. Lee, R. Kaspin *et al.,* "DDoS attack monitoring using smart controller placement in software defined networking architecture," in *Computational Science and Technology. Lecture Notes in Electrical Engineering*, R. Alfred, Y. Lim, A. Ibrahim, P. Antony (Eds.), vol. 481. Singapore: Springer, 2019.

[43] 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.

[44] F. Sattar, M. Hussain and K. Nisar, "A secure architecture for open source VoIP solutions," in *2011 Int. Conf. on Information and Communication Technologies*, Karachi, pp. 1–6, 2011.

[45] 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.

[46] 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.

[47] 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.

[48] R. Singh and G. Soni, "Realization of OFDM based free space optics," in *2015 Int. Conf. on Green Computing and Internet of Things*, Noida, pp. 32–35, 2015.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] N. Salam, M. K. Abbas, M. K. Maheshwari, B. S. Chowdhry and K. Nisar, "Future mobile technology: Channel access mechanism for LTE-LAA using deep learning," in *2021 IEEE 18th Annual Consumer Communications & Networking Conf.*, Las Vegas, NV, USA, pp. 1–5, 2021.

[54] 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 *IEEE 18th Annual Consumer Communications & Networking Conf.*, Las Vegas, NV, USA, pp. 1–6, 2021.

[55] R. Fourer, D. Gay and B. Kernighan, "A mathematical programming language, (AMPL), USA, 2021. [Online]. Available: https://ampl.com.

[56] IBM ILOG CPLEX, "Optimization Studio. New York, USA, 2021. [Online]. Available: https://www.ibm.com/products/ilog-cplex-optimization-studio.

[57] C. Gkountis, M. Taha, J. L. loret and G. Kambourakis, "Lightweight algorithm for protecting SDN controller against DDoS attacks," in *10th IFIP Wireless and Mobile Networking Conf.*, Valencia, Spain, pp. 1–6, 2017.

[58] H. A. Alamri and V. Thayananthan, "Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks," *IEEE Access*, vol. 8, pp. 194269–194288, 2020.

[59] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden and M. Roughan, "The Internet Topology Zoo, Australia," 2021. [Online]. Available: http://www.topology-zoo.org.

[60] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, M. Roughan *et al.,* "Dataset, Australia," 2021. [Online]. Available: http://www.topology-zoo.org/dataset.html.

[61] yWorks, "yEd," Germany, 2021. [Online]. Available: https://www.yworks.com/products/yed.