Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 8, August 2021, pg.23 – 31

Convergence Time Monitoring Algorithm in Hybrid Software Defined Networks

Mawra Gull; Jasdeep Singh
RIMT University, Mandi Gobindgarh, Punjab
DOI: 10.47760/ijcsmc.2021.v10i08.004

Abstract- Network consummation especially dependent on traffic monitoring. Therefore, Software Defined Network (SDN) technology is submitted to support the flow control suitable monitoring by providing a global view of the network. Unfortunately, replacing the entire traditional network to SDN is complex, which leads to the need of SDN switches deployment to the current network. Thus, a hybrid network environment has emerged which consists of centralized controller, SDN switch and legacy routers. Hence, the advantage of the integration of traditional networkand SDN will take place. The controller can collect SDN data instantly, while it waits for a long time to obtain the legacy network data. On the other hand, the rest of paths cannot be processed directly by the controller. Therefore, legacy path load data is estimated for the past time to support the controller for obtaining thecurrent data. The convergence time of the proposed algorithm takes more convergence time than the full SDN by only 12%. Therefore, the proposed algorithm provides installing the minimum possible number of SDN switches that reduce the infrastructure cost.
Keywords: SDN, QOS, MPLS

INTRODUCTION

The undeviating development of Internet speed with a data turnover rate of tens to hundred gigabits per second (Gbps) is observed. Big servers and cloud computing partially solved storing and processing massive data problem. Besides, the sixth version of Internet addresses (IPv6) has solved internet addresses shortage. However, for a reliable, secure, simple, and low-cost network, the infrastructure of the existing network has to be changed. From this point of view, researchers started looking for alternative solutions, then the

emerging technology known as software-defined networking(SDN) was found. It is the next generation of infrastructure in network engineering that supports a traditional network. Therefore, cloud computing, Internet of Things (IoT), big data, and the increasing demands for networks explain our need of SDN [1].

Traditional networks were not designed to handle large amount of data even with increased supply in processing power Ethernet speed, wireless speed, 4G and 5G technologies. The traditional network infrastructure has not changed due to its scalability and stability until SDN emerged in the past few years. However, it encounters some obstacles such as human errors during manual configuration, delay of packets because of distributed control. In addition, the cooperation between two different vendors not exist [2] For example, Cisco protocols are not compatible with Juniper or Huawei protocols. SDN solves the previous problems by the centralization of the controller that provides a global view of the network. Moreover, the centralized point can manage the entire network to minimize errors and provides consistency during configuring rules on the network devices. The SDN centralized controller improves security and quality of service (QoS) through enforcing some safe network rules that limit risks. For example, if any link in the network gets down, the controller instantaneously recognizes the problem, unlike the traditional networks that take a long time to detect the problem [3]. SDN is an effective scheme to save time and effort as well as provides high quality and reliable networks. Hybrid network improves the network performance and facilitates its management where it takes the advantages of both networks.

Therefore, these challenges are solved by the controller centralization, which has a global view of the entire network. Convergence time is the required time for routers to capture each other's information, such as links, devices, and routing tables information. Generally, data packets are handled in similar manner, which may be directed to the same destination and all this occurs in an inexpensive routing device. Moreover, special routing device i.e. ,Cisco router may have the ability to treat different packets depending on their nature and contents. It allows the administrator to mark out priorities of different flows through customized local router programming. Thus, the queue size in each router can manage packets flow directly [4]. Such a customized local router setup allows the operators to handle traffic more efficiently in terms of congestion and prioritization control. The current network devices have the limitation on network performance due to high network traffic, which hinders the network performance in terms of speed, scalability, security, and reliability. The current network devices lack the dynamism in operation, which is related to different types of packets and their contents. It may be attributed to inability to reprogramming of the network operation due to the underlying hardwired implementation of routing 10 rules and various protocols. The goal of SDN is to provide a framework with open, user-controlled management for the forwarding devices in a network [5]. In it, depending upon the scale of the network, the control plane may have one or multiple controllers. In case of multiple controller environments, a high speed, reliable distributed network control can be formed with peer-to-peer (P2P) configuration. In large-scale, high speed computing network, segregation of data plane from control plane plays an important role in SDN, wherein, switches use flow table for packet forwarding in data plane It is due to the fact, that software module (applications) helps administrator to control data flow along with desired change in the characteristics of switching and routing device in network from central location without dealing with each device individually in the network. Control plane Network topology ACLs, forwarding and routing QoS, link management Applications Mobility Management, Access Control, Traffic/Security monitoring, Energy-efficient networking Operating System

API Network Node Data planelink Forwarding Switching, routing a) Conventional approach (each individual network node has its own control and data plane management) Data plane link Forwarding Switching, Routing Control plane Network topology ACLs, forwarding and routing QoS, link management Applications API Network Node[6].

LITERATURE REVIEW

1. Tsai, P.-W., Tsai, C.-W., Hsu, C.-W., & Yang, C.-S.(2018). Network monitoring in software-defined networking: A review. IEEE Systems Journal, 12(4), 3958-3969[7]. In this paper the author explains that to achieve efficient network management, traffic status monitoring is an essential pillar to obtain high quality and stable networks. Network monitoring shows the network behavior status via traffic statistics. With the increased Internet usage and growing a large number of applications, the traditional network suffers from some network performance weaknesses due to a lot of application requirements.

2. Lee, S., Levanti, K., & Kim, H. S. (2014). Network monitoring: Present and future [8]. Computer Networks, 65, 84-98. In this paper the author explains that Traffic matrices are useful for planning and monitoring of network behavior. Therefore, there are two popular methods to monitor traffic flows in real networks, NetFlow application and SimpleNetwork Management Protocol (SNMP). Moreover, SDN is an ideal solution to simplify network monitoring via centralized controller that has a global network view. Network monitoring is divided into two parts: data measurement and data processing.

3.Karakus, M., & Durresi, A. (2017). Quality of service (QoS) in software defined networking (SDN): A survey. Journal of Network and Computer Applications, 80.[9].In this paper the author discusses that network devices are typically consisting of the data plane and control plane. A data plane is the hardware responsible for forwarding packets while the control plane provides the network intelligence such as selecting the best path, setting priorities, and policies. In addition, each device in the traditional network is managed individually and manually, such as a router or switch. However, SDN architecture took out network devices intelligence (control plane) to form a central controller. Therefore, there is a separation between the control and dataplanes of SDN.

4.Amin, R., Reisslein, M., & Shah, N. (2018). "Hybrid sdn networks: A survey of existing approaches,". IEEE Communications Surveys & Tutorials, 48[10]. The control plane is responsible for decision-making such as packet routing, while the data plane executes control plane instructions. The result of separation is that the management function concentrates on a single network device known as the controller, which monitor the network easily.

5.Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software- defined networking (SDN): a survey. Security and communication networks, 9(18), 5803-5833[11]. In this the authors explained that OpenFlow protocol allows control layer to contact with data layer and exchange packet with each other. It has been developed to suit all vendor types. SDN is a more modern approach to manage actions andservices. The network design is one of the prominent advantages that supports different vendors' devices which each other.

6.Amin, R., Reisslein, M., & Shah, N. (2018). "Hybrid networks: A survey of existing approaches,". IEEE Communications Surveys & Tutorials, 48[12]. Vb÷=-0987 In this paper the author explains that the hybrid network is consisting of both traditional and SDN

devices. Accordingly, there are some advantages of integrating both systems so that it facilitates planning, monitoring, and managing the entire network. Moreover, traditional networks could be managed centrally rather than distributed control. In addition, the controller centralization simplifies the management complexity of IP devices, particularly those related to policy configurations and quality of service improvements such as routing policy management, traffic management, and access-list control. on IP addresses as well as multiple sources of control and management. In contrast, SDN controls all devices in a data plane by a single centralized controller. Thus, when both networks are integrated, legacy and SDN systems must be appropriate to communicate with each other, either through software updating or hardware deployment.

7.Sinha, Y., & Haribabu, K. (2017). A survey: Hybrid sdn. Journal of Network and Computer Applications, 100, 35- 55[13]. In this paper describes that Hybrid networks (traditional & SDN) are based on their ability to coexist together, as well as interactivity during communication so that both networks understand each other's functions. The integration of SDN over the traditional network is in three locations, control plane only, data plane only, or both. Merging both networks in data plane only do not provide the network a noticeable benefit. Thus, integrating legacy devices with the controller only or with both controller and SDN devices of the data layer is considered a quantum leap over the traditional network.

8.Caria, M., Das, T., Jukan, A., & Hoffmann, M. (2015). Divide and conquer: Partitioning OSPF networks with SDN. Paper presented at the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)[[14]. First, current devices may not need to be replaced because they provide essential and indispensable services. Besides, it is important to know the adaptability of legacy devices to SDN so that they can interact and communicate with each other. The budget is one of the significant factors affecting the installation of SDNs. Thus, the network planning concerns to install the least possible SDN devices. Also, upgrading the device software may further complicate network management. Factors have encouraged researchers to search hybrid network design solutions. Consequently, twomechanisms were introduced for SDN deployment.

9.Joglekar, C. A. (2017). Route Manipulation using SDN and Quagga. The author explains the Mininet Emulator is a tool used for software-defined networks[15]. It provides hosts, open-flow switches, and controllers by using CLI. A pure SDN can be established which represents a real network. The emulator runs only on the Linux system, but it can be used on other systems via virtual programs such as VMware. The Mininet checks and tests the SDN structure efficiency. In order to simulate the hybrid network in Mininet, it requires to install Quagga software over the Linux system.

PROBLEM FORMULATION

SDN is the optimal solution for traditional network shortcomings. However, it is very costly to migrate from the traditional network to SDN immediately. Therefore, SDN devices are deployed gradually into legacy devices. There are numerous studies being carried out about monitoring on pure SDN and traditional networks. However, the monitoring in hybrid networks is still under- research due to a lack of studies in this field.

It is not easy to achieve full traffic management such as load balance, congestion, and latency for hybrid SDN because the entire network is not under single control. The

centralized controller of SDN can easily manage OpenFlow switches and recognize the paths status in real time. Due to multiple Interior Gateway Protocol (IGP) routers in the traditional network part, collecting path load state data for large-scale network topology takes long time. Thus, paths monitoring is a critical issue.[16]. It is important to speed up the convergence time to help the controller to make decisions promptly when dealing with any changes in the network.

RESEARCH METHODOLOGY

The enhancement of the network convergence time consists of four phases:

i. Gathering paths status data from the traffic matrix.
ii. Determine the most critical paths that may cause latency.
iii. Replacing legacy routers that cover the critical paths to SDN switches.
iv. Estimation of the state path using the data generated from the previous data path.

Generating Traffic Matrix

The traffic matrix is extremely supportive in monitoring the path state and protects themthe path state from any issue [38]. Monitoring a traditional network requires significant efforts to achieve high network performance. On the other hand, the SDN came up to optimize the traffic monitoring performance. Real traffic flow data of ISP network is not allowed to be published due to security and competitive issues. Therefore, it is hard to find ISP networks public traffic matrix. Traffic matrices are generated over the network by using Fast Network Simulation Setup (FNSS) module of Python [33]. FNSS in addition applies link parameters such as capacity, delay, and weight. Traffic matrix shows the traffic between each two devices.

Choosing Critical Paths

In ISP networks, few paths contain high traffic flows, while the rest do not [7]. Network management relies primarily on monitoring paths status. The proposed algorithm is based on deploying the smallest possible number of SDN switches in the appropriate locations to collect the complete network information through SDN switches only. The SDN switches supply the controller by information in real-time. Hence, the controller makes quick decisions accordingly. The path traffic amount can be found from the traffic matrix content while routing matrix determines the place of each traffic. Load matrix (M) consists of total number of paths, i.e. columns (m), and sequential time, i.e. rows (n) such as number of months, weeks, or days. Analyzing path load data requires todecompose the load matrix using Singular Value Decomposition (SVD) tool. After applying SVD on path load matrix, Permutation matrix (P) is used to arrange all matrix columns (paths) from the largest singular value to zero. It shifts critical paths to the beginning of the matrix (M). Therefore, path load data of all network can be gathered by using only critical paths. Equation below shows paths order where $M1$ represents the critical paths, while $M2$ shows legacy paths.

$$MP = [\underbrace{M_1}_{k} \vdots \underbrace{M_2}_{m-k}]$$

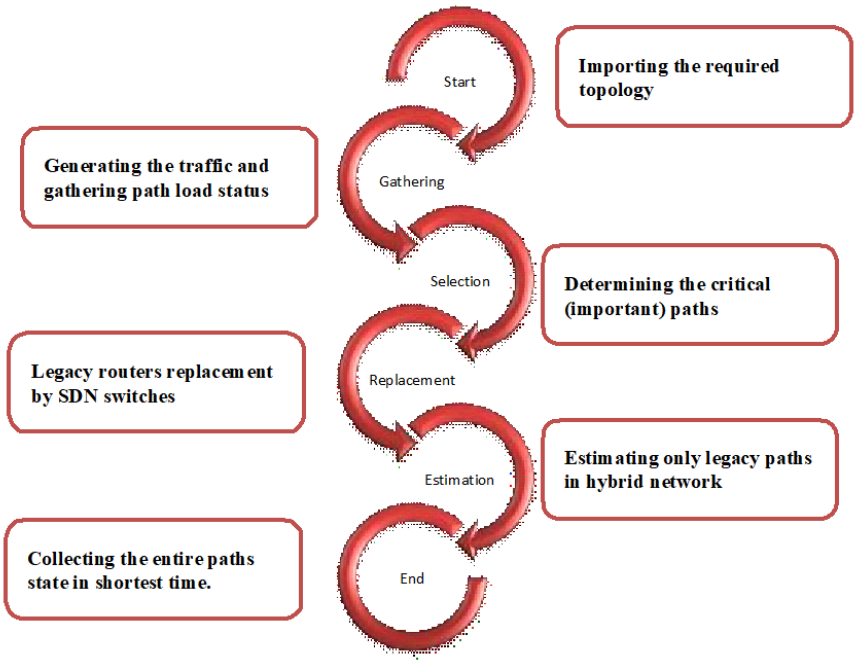
Legacy Routers Replacement

ISP topology consists of pure legacy routers where a distributed control manner takes place. Thus, critical paths must be covered by SDN switches. A legacy router gradually will be replaced by SDN switch depending on the critical paths number connected into legacy routers exist. Consequently, SDN switches deployment improves network monitoring and management. The controller can manage the most valuable part of the network i.e. critical paths. In this way, the controller immediately can collect paths status data covered by SDN switches., while legacy routers remain in contact with SDN switches. The critical paths covered by the legacy router are computed first, then the most critical paths connected to the router are selected. Consequently, legacy router is replaced by the SDN switch. Finally, new topology is updated, and the process of covering by SDN switches will be repeated as long as the critical paths.

Estimating Legacy Path Load

Controller receives data from SDN switches so that routers exchange packets with switches via LSPs. The network crucial information can be obtained through critical paths in real-time. On the other hand, the controller requires to estimate rest paths status for the present period . Critical path state data can be obtained in the current period, while legacy paths load state can be achieved by estimating current load data based on past period data [7]. Therefore, the entire paths state can be gathered in real- time.

These steps are shown in Figure below:



Research Methodology Flowchart

RESULT ANALYSIS AND DISCUSSION

This presents the simulation result analysis of the proposed monitoring algorithm. Results highlight the impact of SDN switches and legacy path load estimation to improve the latency between legacy routers and the controller. Comparison of the monitoring algorithms performance among full SDN, randomly SDN switches, and the proposed algorithm in hybrid network is evaluated.

REQUIRED SDN SWITCHES

The proposed architecture consists of 24 routers and 72 paths. Thus, the relationship between the chosen critical paths and required number of SDN switches to cover criticalpaths is evaluated as shown in Figure 4.1.

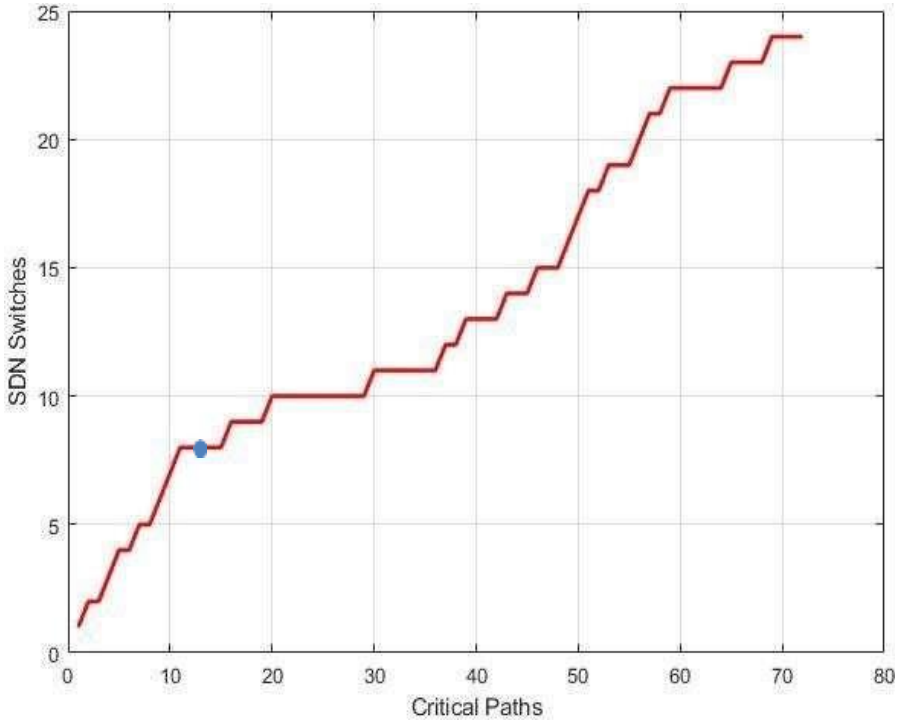


Figure 1.2 Relation Between Critical Path and SDN Switches

Paths number is increased from 1 to 72 to compute the number of needed SDN switches. In this case, 13 critical paths require 8 SDN switches. The point in Figure.4.1 shows that the 13 critical paths require 8 SDN switches. The more critical paths number, the more SDN switches needed to manage and control those paths efficiently. Locating SDN switches is an advantage of the proposed algorithm. Hence it provides a minimumnumber of SDN switches which saves cost and other associated overhead issues.

LEGACY LOAD ESTIMATION

According to Equation 3.4, to obtain total load data instantly, the controller collects current SDN load data and estimates the past legacy path load data. The number of critical paths in this study is 13 paths, as mentioned in Chapter 3. Thus, rest paths are necessary to be estimated by the controller. Consequently, the estimation accuracy of legacy path load data is evaluated in Figure 4.2. It shows the relation of critical paths using SDN technology and legacy paths estimation.

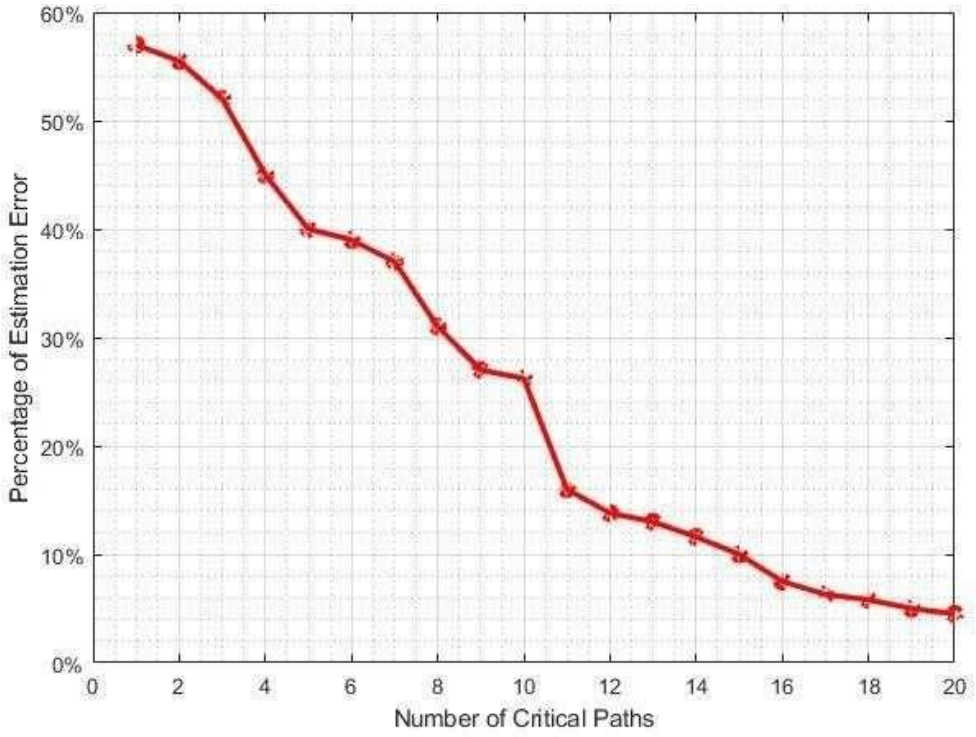


Figure 1.3 Estimation Accuracy of Legacy Path Load

The lower legacy paths are the more precise load estimation rate. The proposed monitoring algorithm displays an estimated error rate of around 14%. This percentage is sufficient to obtain semi-accurate of the full path data. One of the constraints to accurate load estimation is the increase in the number of legacy paths.

CONCLUSION

The increase in data usage due to the emergence of new technologies made it more difficult to handle large amount of data by the traditional network. Thus, Software Defined Network (SDN) has come up to address these problems. On the other hand, it is not possible to migrate to SDN directly where SDN switches deployment will gradually take place in the network. Thus, a hybrid network environment has emerged consisting of a central controller, SDN switches, and legacy routers. The controller collects the SDN path load data instantly, while it takes a long time to obtain the legacy path load data. Consequently, failure detection and traffic management cannot be recognized in real-time. The main objectives of this research are to replace minimum number of legacy routers that reduce cost and convergence time. These objectives are made by proposing the algorithm to monitor path load data and selects significant paths to be covered by SDN switches using Singular Value Decomposition (SVD). Moreover, minimum possible number of SDN switches were installed to cover the critical paths. Legacy path load data is estimated for the past time to support the controller for obtaining the current data. It has been observed that the convergence time of the full SDN is better than the proposed monitoring algorithm by only 12%. Moreover, the proposed algorithm reduces a number of SDN switches used. Finally, the proposed algorithm has demonstrated noticeable improvement in traffic management by 11% compared to full SDN.

REFERENCES

[1]. Abushagur, A. A., Chin, T. S., Kaspin, R., Omar, N., & Samsudin, A. T. (2019). *Hybrid Software-Defined Network Monitoring.* Paper presented at the International Conference on Internet and Distributed Computing Systems.

[2]. Akyildiz, I. F., Lee, A., Wang, P., Luo, M., & Chou, W. (2014). A roadmap for traffic engineering in SDN-OpenFlow networks. *Computer Networks, 71*, 1-30.

[3]. Amin, R., Reisslein, M., & Shah, N. (2018). "Hybrid sdn networks: A survey of existing approaches,". *IEEE Communications Surveys & Tutorials*, 48.

[4]. Barreto, F., Wille, E. C., & Nacamura Jr, L. (2012). Fast emergency paths schema to overcome transient link failures in ospf routing. *arXiv preprint arXiv:1204.2465*.

[5]. Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. *Security and communication networks, 9*(18), 5803-5833.

[6]. Caria, M., Das, T., Jukan, A., & Hoffmann, M. (2015). *Divide and conquer: Partitioning OSPF networks with SDN.* Paper presented at the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM).

[7]. Cheng, T. Y., & Jia, X. (2017). Delay-sensitive multicast in inter-datacenter WAN using compressive latency monitoring. *IEEE Transactions on Cloud Computing*.

[8]. Cheng, T. Y., & Jia, X. (2018). Compressive Traffic Monitoring in Hybrid SDN. *IEEE Journal on Selected Areas in Communications, 36*(12), 2731-2743. doi:10.1109/JSAC.2018.2871311.

[9]. Coates, M., HERO, A., Nowak, R., & Yu, B. (2002). Internet tomography IEEE Signal Processing Mag., v. 19. In: May.

[10]. Coates, M., Pointurier, Y., & Rabbat, M.(2007). Compressed network monitoring for IP and all-optical networks.

[11]. De Oliveira, R. L. S., Schweitzer, C. M., Shinoda, A. A., & Prete, L. R. (2014). *Using mininet for emulation and prototyping software-defined networks.* Paper presented at the 2014 IEEE Colombian Conference on Communications and Computing (COLCOM).

[12]. Fan, X., & Li, X. (2017). Network tomography via sparse Bayesian learning. *IEEE Communications Letters, 21*(4), 781-784.

[13]. Fan, X., Li, X., & Zhang, J. (2018). Compressed sensing based loss tomography using weighted ℓ1 minimization. *Computer Communications, 127*, 122-130.

[14]. Guo, Z., Chen, W., Liu, Y.-F., Xu, Y., & Zhang, Z.-L. (2019). Joint Switch Upgrade and Controller Deployment in Hybrid Software-Defined Networks. *IEEE Journal on Selected Areas in Communications, 37*(5), 1012-1028.

[15]. Hartung, M., & Körner, M. (2017). SOFTmon-traffic monitoring for SDN. *Procedia Computer Science, 110*, 516-523.

[16]. Hong, D. K., Ma, Y., Banerjee, S., & Mao, Z. M. (2016). *Incremental deployment of SDN in hybrid enterprise and ISP networks.* Paper presented at the Proceedings of the Symposium on SDN Research.

[17]. Huang, S., Zhao, J., & Wang, X. (2016). *Hybridflow: A lightweight control plane for hybrid sdn in enterprise networks.* Paper presented at the 2016 IEEE/ACM 24th International Symposium on Quality of Service (IWQoS).

