Comparative Analysis of SDN and Conventional Networks using Routing Protocols

Deepthi Gopi[2], Samuel Cheng[1,2] and Robert Huck[2]
[1]Department of Computer Science and Technology
College of Information Engineering
Tongji University, Shanghai, China 201804
Email: szeming@tongji.edu.cn
[2]School of Electrical and Computer Engineering
University of Oklahoma-Tulsa, Tulsa, Oklahoma 74135-3324
Emails: [deepthi, samuel.cheng, rchuck]@ou.edu

***Abstract*—Conventional routing protocols such as RIP, OSPF, EIGRP and BGP have a very rigid and intricate system thus narrowing the adaptability of networks to the ever changing Internet. The emergence of Software Defined Networking (SDN) provides a solution for this problem. Due to the handiness of a centralized controller, SDN has provided an effective method in terms of routing computation and fine control over data packets. Due to the increase in unpredicted failures taking place the ability to predict/know the approximate maximum time it takes for these networks to converge in order to avoid and/or minimize loss of packets/data during these failures has become crucial in today's world. This time that the routers in the network take to converge via the implemented routing protocol and resume communication or transfer of information is called the routing convergence time.**

In this work, the performance is measured using routing convergence time during link failure with respect to the topology scale to show that SDN routing/forwarding is better compared to conventional routing. Further the results indicate that the routing convergence time is less in SDN networks on comparison with conventional networks when the topology scale is increased, indicating that SDN networks converge faster in comparison with Conventional networks and that routing convergence time is greatly influenced with the changing topological size.

***Index Terms*—Software Defined Networks (SDN), Conventional Networks, Border Gateway Protocol (BGP), OpenFlow Protocol, Convergence process, Routing Convergence Time, Topology Size, Routing Protocols.**

I. Introduction

The Internet has a very deep relationship in every nook and corner of our lives. The routing protocols play a very important role in TCP/IP communication. The data packets sent from the source traverse through the Internet constituting routers, switches, etc. to reach their respective destination. When a link/node failure occurs, the job of these protocols is to quickly detect link failure and find an alternative route to reach the destination [1].

With the growth in unforeseen failures and attacks, the ability of failure detection and recovery has become critical in today's world. Similarly the need to transfer information from a source to a given destination during link failures or when changes in the topological information occur is also very crucial. Given a circumstance, it is important to be able to predict/ know the approximate maximum time it takes for a network to converge in order to avoid and/or minimize loss of packets/data [1], [2]. Routing convergence time is considered as one of the vital performance indicator and design goal for determining the performance of the routing protocol [3] and is of prime importance for networks, the faster the routers running the protocol help the network to converge during failure the more reliable it is to be used in real time applications [4].

978-1-5090-5957-7/17/$31.00

In SDN, the control plane (network plane) and the data plane (forwarding plane) are decoupled thus enabling direct provision of programming the network plane [5], [6]. Due to the presence of the controller in SDN networks, the controller transfers the control power of the data packets [2], [6] from the data plane switches to the central controller thus stipulating faster convergence in comparison to conventional networks. We know, from the reference [9] that the size of the network (topology size) plays a significant role in routing convergence time, a larger network will converge slower than a smaller one. Likewise, in [10], [11] where they compared convergence time for different network sizes w.r.t time function and the results showed a logarithmic relationship between topology size and routing convergence time in peer-to-peer (P2P) networks, there was a consistent change in the convergence time with continuous increase in network size. Thus, in this paper, we study the performance of SDN and conventional routing with respect to routing convergence time and increase in topological size.

II. Related Work

Many papers in past indicate research in comparative study of routing convergence time of different routing protocols for conventional networks and analyzing which routing protocol has the least routing convergence time/which routing protocol converges faster and how it will affect the performance of the networks. D. Sankar et al. 2013 used OPNET simulation tool and real equipment to compare the convergence duration of routing protocols RIP, OSPF and EIGRP in conventional networks, and analyzed how it would affect the packet loss

and quality of real time application [3]. From this work, they drew conclusions that in both using simulation and real time the convergence for EIGRP is much faster compared to OSPF and RIP whereas RIP took the longest time to converge in both the scenarios. Similarly, reference [7] discusses the process of choosing the routing protocols (involves distance vector/link state or both) by capturing the traffic generated by each of the protocols and analyzing it, the conclusion drawn was convergence time of OSPF was faster than others.

In [8], they developed a model which could achieve better network convergence based on the traffic variations thus improving network dependency and traffic performance. Along similar lines, from [12], they used SSFNet simulator to build conventional networks where they tried to investigate the relationship between BGP routing convergence time and the configuration of the Minimum Route Advertisement Interval (MRAI) timer for every simulated conventional network topology. Likewise, in [2] they studied ping response time w.r.t to varying packet forwarding delay using Open Shortest Path First (OSPF) protocol and OpenFlow protocol to study the behavior of routing convergence time performance [2].

Up to now, most of the papers which have been discussed previously have tried to study, assess and analyze the routing convergence time of dynamic routing protocols only in the conventional networks. We believe that our study can throw light upon many advantages in SDN with regards to faster convergence during node and link failures in contrast to archaic conventional networks, thus the main contributions of this paper are evaluating/comparing the performance of two different technologies namely SDN routing/forwarding using OpenFlow protocol and conventional routing using Border Gateway Protocol (BGP) with respect to routing convergence time and topological size. On comparison we study the convergence time behavior with different network sizes i.e. continuous increase in network topology size.

The remainder of this paper is organized as follows. Section 3 introduces the concept of convergence and the importance of routing convergence time. Section 4 describes the software tools used, topologies, experimental scheme and settings. Section 5 presents the BGP routing and SDN routing mechanism discussing in terms of routing convergence time along with summarizable results is demonstrated. The paper is concluded in Section 6 with outcomes and graphs along with future research work.

III. Convergence Analysis

A. Convergence Process

Convergence is defined as the state in which the routers come to an agreement on the best paths for sending packets to the destination thus in turn completely updating their routing tables and possessing similar topological intelligence about the network in which they function [16], [17]. For the routers operating on dynamic protocols in a network, convergence is an essential parameter to operate correctly [18]. Whenever a link or node failure occurs, basically any change in the topology of the network gives rise to convergence. During convergence every router will independently re-compute alternative paths and construct a new routing table based on the new information attained, once these tables have been updated with the changes, convergence is completed and the transfer of data packets resumes from the source to destination [13], [14], [16]. The data attained by the routers must not conflict with any other router's routing table information, they must possess the correct topology information exchanged with each other [19], [20]. A network is said to be converged if the routers know how the network looks like, which links are up/down and which are the best routes to reach every destination [7], [15]. The concept of convergence helps in planning for network capacity, service capacity and criticality of infrastructure mainly in terms of network designing in order to avoid network overloading or suspicious attacks leading to instability and uncertainty [16], [21].

1) Routing Convergence Time: The time the routers take to come to an agreement with regards to the new topology after their routing tables are completely updated is called routing convergence time.

From [22], it describes routing convergence time as the sum of failure detection time, flooding of information time, processing the routing updates time, computating paths time and alternative/rerouted path installation time.

It depends on topology size i.e. the number of routers using the routing protocols within the network, distance of routers (from point of link failure), bandwidth and traffic load on the network links, static/dynamic routing protocol used [9], [16].

IV. Experiment settings and software tools used

For SDN networks, we use Floodlight [35] controller as the main controller for the network, Mininet (a network simulator) [33], [34], [35] is used to create the network consisting of switches, routers and hosts [2], [33] as well as to measure the routing convergence time. For conventional networks, we use Packet Tracer (network simulation and visualization tool) for creating the network consisting of switches, routers and hosts enabling manual programming of routing protocols in the routers. In both networks, the real timer (ms), ping and traceroute commands are used for measuring the routing convergence time. In this work, using Mininet network simulator we have created 3 topologies: 8 nodes, 16 nodes and 80 nodes with 2 hosts for conventional networks and SDN networks. The routers in the conventional network are manually configured with BGP protocol and assigned appropriate AS (Autonomous System) numbers. In SDN network, all the switches in the network are directly connected to the controller. The topology diagrams are shown below:

1) Experimental Scheme: In this work, first a stable communication is established between host 1 (H1) and host 2 (H2) using the ping command, once this is achieved using traceroute command the main path is detected as shown in Figure 4, the Link 1 as shown in Figure 1 is broken down and the routing convergence time is recorded during this period then the link is restored back up and the same process is repeated 50 times, finally taking the average of all the readings. Likewise, this

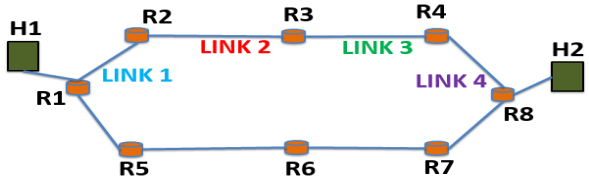


Figure 1: 8 nodes topology

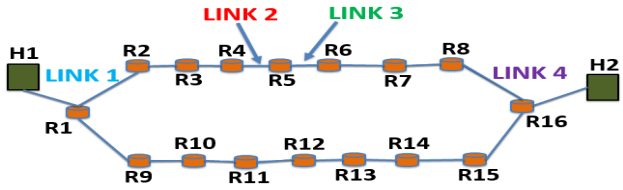


Figure 2: 16 nodes topology

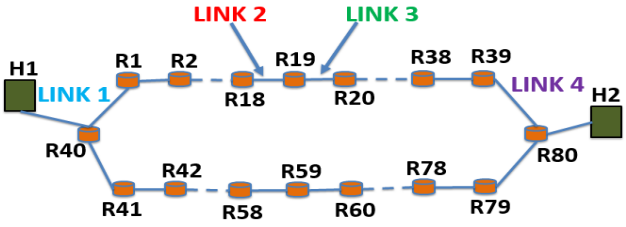


Figure 3: 80 nodes topology

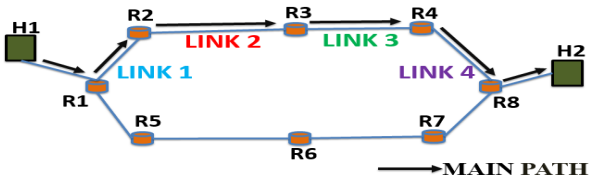


Figure 4: 8 nodes topology indicating the Main Path

process is repeated for links at different positions (Link 2, 3 and 4) for the given networks with different topology sizes as shown in Figure1, 2, 3 and 4.

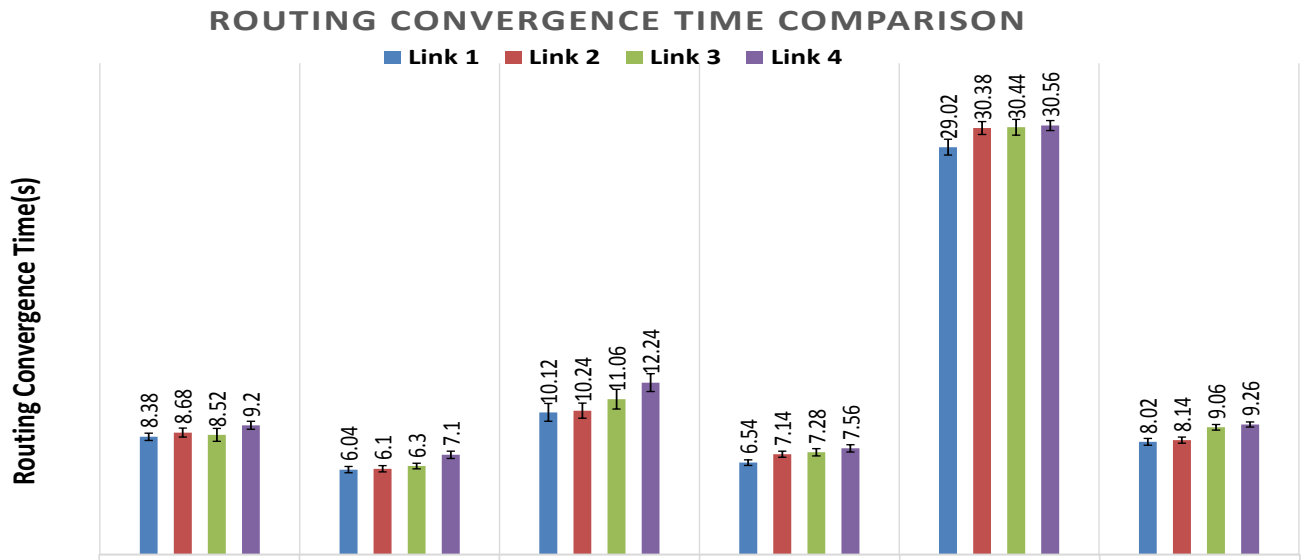
V. Results and Analysis

In the simulation experiment, the bandwidth is set as 10 Mbps and link delay is 0 ms to calculate the routing convergence time. Figure 5 also shows the table which indicates the various values obtained for routing convergence time at different link positions for both conventional and SDN networks.

From Figure 5 we see that the routing convergence time of SDN networks is lesser compared to Conventional Networks for all the three topologies. The explanation for this phenomenon lies in the convergence process of SDN and conventional networks. We can deduce from the graph in Figure 5 the following two outcomes/results, the first result is explained below:

In Conventional Networks, when a routing change occurs (e.g., a link is down, etc.), it will take some time for R1 to realize that the connection is no longer valid [23].
1) R1 will first remove the invalid routes from its routing and forwarding tables, then it sends BGP MESSAGE updates to its neighbors to inform them about the link down [23].
2) When the neighboring AS will receive these updates, it will calculate and change any needed updates (if any are there) for its routing table, it will in turn send updates (with withdrawal messages) to its own neighbors withdrawing the lost routes. Thus, the BGP updates will propagate over the entire network in this way [24], [25], [26].
3) The withdrawal updates are processed by the neighbors, they will choose the alternate best paths, and add these paths to their own routing and forwarding tables (FIB and RIB tables) [24], [25], [26], [12].
4) Then the neighbors will broadcast their new best paths. The router processes incoming BGP updates, elects new best paths, and adds them in routing and forwarding tables and continues to propagate these updates to other ASes [24], [25], [26].
5) Once a new path is elected then the connection is established and transfer of information resumes [24], [25], [26].
The causes of delayed convergence time is because the failure detection and propagation by means of BGP mechanics is slow, and depends on the number of affected prefixes. The process of uploading both the RIB and FIB updates are time-consuming and the new information obtained is always been compared with the local routing table information on a consistent basis thus further causing delayed routing convergence time [12], [24], [25], [26].
Therefore, in BGP if the damage is severe, the information about it is transmitted at a slow pace.

Whereas, in SDN networks, the controller sets the configuration parameters of the switch through the SET_CONFIG [28] message during the primary phase of the controller-switch dialogue. The controller supervises the switch via the OpenFlow protocol. The controller can add, update, and delete flow entries [28] using this protocol, here a flow is a set of packets transferred from one network endpoint to another endpoint.
1) Whenever a failure occurs in a network like port down/link failure/neighbor fails, the SDN switch will first detect that a failure has occurred through PORT_STATUS [27], [28].
2) The switch uses the ERROR message to notify the controller about the failure by sending a message to the controller [28].
3) Once controller is notified about a failure the controller will use the knowledge of the entire network to compute new flows which do not use the failed component during transfer [27]. The controller chooses the rerouted/alternate path from the flow tables.



	Conventional Network (8 node)	SDN Network (8 node)	Conventional Network (16 node)	SDN Network (16 node)	Conventional Network (80 node)	SDN Network (80 node)
Link 1	8.38	6.04	10.12	6.54	29.02	8.02
Link 2	8.68	6.1	10.24	7.14	30.38	8.14
Link 3	8.52	6.3	11.06	7.28	30.44	9.06
Link 4	9.2	7.1	12.24	7.56	30.56	9.26

Figure 5: Routing Convergence Time comparison

4) Using the FLOW_MOD message, the controller changes the current flow entries in the switch such that all flows will avoid the failed element such that the switch that identified the failure will reroute the flows [28].
5) Using the FLOW_MOD(MODIFY) command [28] controller seeks to modify the corresponding flow entry where the MODIFY command will notify the switch to change/modify the field headers like VLAN headers, Ethernet source and destination address, and IPv4 source and destination address [28] may be changed.
6) The controller will update its own flow table information and then pushes the same data onto the switch in the network.
7) Switches which are affected by the failure will receive the updated flow table information from the controller and will in turn update their flow tables with the information received [27].
8) Next when a packet enters the switch, the switch matches the packets header field with its new flow table information, if a match is found in the flow table then it forwards the packet out to the necessary local port. If the packet does not match the flow entry then the packet is dropped or passed to the controller for further processing [28].
Basically the controller performs the routing convergence work in the SDN network and the routing convergence time in SDN networks depends on link down detection, topology message update time (from controller to switch) and flow table update time [2].

In the second result we see that, the convergence time keeps increasing as the topology size increases from 8 to 80 nodes, this occurs because when there is a change in a network then the conventional network must send updates to all the routers via BGP protocol to update the routing tables through the links. Flooding [29], [30], is similar to broadcasting, it is a way of distributing routing information updates quickly to every node in a large network [29], [30]. Thus, the information of the failed link is propagated through flooding. Flooding, of course, scales linearly with topological scale since it uses every path in the network [31]. Thus, as the topology size/number of routers keeps increasing, the protocol has to send updates and advertise new routes to all the routers, withdraw all the failed routes from all the routers in the network and also the routers in the network take time to update their own RIB and FIB tables in turn affecting and enhancing the routing convergence time [2].

In SDN networks, instead of flooding the information about all the routing updates over the entire network, the only device which is updated about the link failure is the controller [2], thus the routing convergence time is less affected in this case. The controller calculates/finds the rerouted path andl pushes the rerouted path information to the affected switches. Next when a packet enters the switch, the switch matches the packets header and forwards the packet out to the necessary local port [2], [32]. If no match is found in a flow table, the default is to forward the packet to the controller over the OpenFlow channel or to drop the packet [28].

VI. Conclusion

In this paper, we conclude that when there is a change in a network like link/node failures the routing convergence time in conventional networks continues to increase with increase in topology scale, because the information of the failed link/node is propagated through flooding in order to update all the routing tables of the routers. Since flooding scales linearly with topology scale, it affects the routing convergence time. Routing convergence time is also greatly influenced by the following parameters: failure detection and propagation, BGP message update time, FIB and RIB update time, withdrawal process (of lost routes) and advertising new routes to neighbors in BGP protocol.

In case of SDN networks, with increase in topology scale there is not much significant change in routing convergence time. Since the controller performs the routing convergence work and the topology information of the network is not maintained by the switches, when there is a change in the network instead of being flooded the information goes to the controller, which sends the updated routing tables to the affected switches and doesn't have to update the information to all the devices in the network so the routing convergence time is not much affected and moderately stable. The routing convergence time in SDN networks depends on: link down detection, topology message update time (from controller to switch) and flow table update time.

References

[1] Gotz Lichtwald, Uwe Walter and Martina Zitterbart, "Improving Convergence Time of Routing Protocols," March 2004. *In Proceedings of 3 International Conference on Networking (ICN'04)*.

[2] Hailong Zhang and Jinyao Yan, "Performance of SDN routing in comparison with Legacy routing protocols," September 2015. *In Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2015 International Conference on (pp. 491-494). IEEE*.

[3] D. Sankar and D. Lancaster, "Routing Protocol Convergence Comparison using Simulation and Real Equipment," *Advances in Communications, Computing, Networks and Security, 10(2013), pp.186-194*.

[4] Joseph Kobina Panford, Kwabena Riverson, Boansi Kufuor Oliver and Rasheeda Mendeeya Yehuza, "Comparative Analysis Of Convergence Times Between RIP And EIGRP Routing Protocols In A Network," April 2015. *Researchjournali's journal of computer science, Vol. 2, no. 3 April 2015, ISSN 2349-5391 pp.1-10*.

[5] Ramos Kreutz, Fernando MV Ramos, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky and Steve Uhlig, "Software-defined networking: A comprehensive survey," 2015. *Proceedings of the IEEE 103, no. 1 (2015): 14-76*.

[6] Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," 2014. *IEEE Communications Surveys and Tutorials 16, no. 3 (2014): 1617-1634*.

[7] Mustafa Abdulkadhim,"Routing Protocols Convergence Activity and Protocols Related Traffic Simulation With It's Impact on the Network," 2015. *International Journal of Science, Engineering and Computer Technology 5, no. 3 (2015): 40*.

[8] Dan Zhao, Hongjun Liu, Xiaofeng Hu and Chunqing Wu, "Towards network convergence and traffic engineering optimization," 2012. *In Performance Computing and Communications Conference (IPCCC), 2012 IEEE 31st International, pp. 448-455. IEEE, 2012*.

[9] Sumit Kasera and Nishit Narang, Communication networks: principles and practice. Tata McGraw-Hill Education, 2005.

[10] Sven A. Brueckner, Giovanni Di Marzo Serugendo and David Hales,"Engineering Self-Organising Systems," *Third International Workshop, ESOA 2005, Utrecht, The Netherlands, July 25, 2005, Revised Selected Papers. Vol. 3910. Springer, 2006*.

[11] Mark Jelasity and Ozalp Babaoglu, "T-Man: Gossip-based overlay topology management," 2005. *In International Workshop on Engineering Self-Organising Applications, pp. 1-15. Springer Berlin Heidelberg, 2005*.

[12] Timothy G. Griffin and Brian J. Premore, "An experimental analysis of BGP convergence time," 2001. *In Network Protocols, 2001. Ninth International Conference on, pp. 53-61. IEEE, 2001*.

[13] Sahrish Khan, Abdul Wahid and Sadaf Tanvir, "Comparative study of routing strategies in software defined networking," 2016 *In Proceedings of the 31st Annual ACM Symposium on Applied Computing, pp. 696-702. ACM, 2016*.

[14] Jonathan Wellons, Liang Dai, Yuan Xue and Yi Cui,"Predictive or oblivious: a comparative study of routing strategies for wireless mesh networks under uncertain demand," 2008 *In Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on, pp. 215-223. IEEE, 2008*.

[15] Wolfgang Braun and Michael Menth, "Software-defined networking using OpenFlow: Protocols, applications and architectural design choices," 2014 *Future Internet 6, no. 2 (2014): 302-336*.

[16] Convergence definition by The Linux Information Project, http://www.linfo.org/convergence.html.

[17] H. Berkowitz, E. Davies, S. Hares, P. Krishnaswamy and M. Lepp, "Terminology for benchmarking bgp device convergence in the control plane. No. RFC 4098. 2005."

[18] John P. John, Ethan Katz-Bassett, Arvind Krishnamurthy, Thomas Anderson and Arun Venkataramani,"Consensus routing: The Internet as a distributed system," 2008 *In Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, pp. 351-364. 2008*.

[19] Patricia A. Morreale and James M. Anderson, Software Defined Networking: Design and Deployment. CRC Press, 2015.

[20] David Kim and Michael G. Solomon, Fundamentals of information systems security. Jones and Bartlett Learning, 2016.

[21] James G. Stavridis, Convergence: illicit networks and national security in the age of globalization. Edited by Michael Miklaucic, and Jacqueline Brewer. Government Printing Office, 2013.

[22] Amir Siddiqi and Biswajit Nandy, "Consensus routing: The Internet as a distributed system.Improving network convergence time and network stability of an OSPF-routed IP network," 2005 *In International Conference on Research in Networking, pp. 469-485. Springer Berlin Heidelberg, 2005*.

[23] Pavlos Sermpezis and Xenofontas Dimitropoulos,"Can SDN Accelerate BGP Convergence?A Performance Analysis of Inter-domain Routing Centralization," 2017. *arXiv preprint arXiv:1702.00188 (2017)*.

[24] Petr Lapukhov, Understanding BGP Convergence. http://blog.ine.com/2010/11/22/understanding-bgp-convergence/

[25] BGP CONVERGENCE OPTIMIZATION, https://www.ipspace.net/BGP _Convergence _Optimization.

[26] BGP Routing Table Analysis REPORTS, http://bgp.potaroo.net/

[27] Naga Katta, Haoyu Zhang, Michael Freedman and Jennifer Rexford,"Ravana: Controller fault-tolerance in software-defined networking," 2015 *In Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research, p. 4. ACM, 2015*.

[28] Paul Goransson, Chuck Black, and Timothy Culver, Software Defined Networks: A Comprehensive Approach. Morgan Kaufmann, 2016.

[29] What is flooding? - Definition from WhatIs.com - SearchNetworking, http://searchnetworking.techtarget.com/definition/flooding.

[30] What is Flooding? - Definition from Techopedia, https://www.techopedia.com/definition/16190/flooding-networking.

[31] Joseph P. Macke and Justin W. Dean, "A study of link state flooding optimizations for scalable wireless networks," 2003 *In Military Communications Conference, 2003. MILCOM'03. 2003 IEEE, vol. 2, pp. 1262-1267. IEEE, 2003*.

[32] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker and Jonathan Turner, "OpenFlow: enabling innovation in campus networks", 2008 *ACM SIGCOMM Computer Communication Review 38, no. 2 (2008): 69-74*.

[33] Casimer DeCusatis, Aparicio Carranza, and Jean Delgado-Caceres, "Modeling Software Defined Networks using Mininet," *Proceedings of the 2nd International Conference on Computer and Information Science and Technology (CIST16) Ottawa, Canada, May 11 12, 2016 Paper No. 133.*

[34] Mininet: An Instant Virtual Network on your Laptop (or other PC) - Mininet, www.mininet.org/walkthrough/

[35] Floodlight OpenFlow Controller - Project Floodlight, www.projectfloodlight.org/floodlight/