DJ Journal of Advances in Electronics and Communication Engineering, Vol. 2(1) 2016, pp. 1-9

REVIEW ARTICLE

An Extensive Review on Software Defined Networking (SDN) Technologies

*Y.R Medlin Benisha[1]

[1]St. Xavier's Catholic College of Engineering, Chunkankadai, Nagercoil, Kanyakumari District, 629003, Tamil Nadu, India.

Received-1 December 2015, Revised-31 December 2105, Accepted-18 January 2016, Published-29 January 2016

ABSTRACT

In the present days, network technologies have always been an important part of success in any communication system. The internet has led to a digital society formation, where from anywhere almost everything is linked and is easily reached. Despite their widespread adoption, traditional IP networks are intricate and very hard to manage. According to predefined policies, it is hard to both configure and reconfigure the network in the case of response to faults, loads and changes. This can lead to problems in effectiveness due to the slow scalable IT infrastructure growth. In this paper, an extensive review on Software Defined Networking (SDN) is presented. Response to problems by providing novel functions to the entire network topology can be easily carried out with SDN. With software defined networking, administrators have the opportunity to abstract the underlying infrastructure of the network for applications and services. After introducing SDN, key concepts and its traditional networking differences, its roots and the activities of standardization are explained in an attempt to expect the future growth of this new model and discuss the main on-going research attempts and challenges. We formulate a scenario classification in which these technologies may contact and observe a significant degradation in the web services performances, in terms of response time and availability. At last we analyse the SDN position as the main enabler of a software-defined environment. SDN present novel networking ideals, simplifying management of network and facilitating evolution in network.

Keywords: Network technologies, Traditional network, IP networks, Control planes and data planes, Reactive routing

1. INTRODUCTION

The term SDN (Software-Defined Networking) also called Software-Driven Networks was originally coined to signify the thoughts and work around open flow [1]. As originally defined, SDN refers to an architecture of network where remote control plane is decoupled and managed from the former state of forwarding in the data plane. The industry of networking has in many cases shifted from this SDN original view, by mentioning to anything that includes software as being Software-Defined Networking (SDN).

2. OVERVIEW AND METHOD OF SDN ARCHITECTURE

Software-Defined Networks (SDN) are used to provide management flexibility and mechanisms of programmability introduced by automation to the network components. These mechanisms are required to permit the network to react faster and to enable them in applying variations to the logical topology when it is required to cover particular necessities. The control logic and the data logic are decoupled from network devices in the architecture of SDN, unlike the architecture of traditional networks. The logically centralized controller is combined by the control plane. It keeps the global observation of the whole network and makes it programmable using applications of software running on top of it. Advantages of SDN are network operators, administrators and researchers. Furthermore, it provides a managed network abstraction to the applications of the controller and also offers reactive routing. The logical topology of reactive routing is continuously developing

*Corresponding author. Tel.: +919488382544
Email address: 21benisha@gmail.com (Y.R.M.Benisha)
Double blind peer review under responsibility of DJ Publications
http://dx.doi.org/10.18831/djece.org/2016011001

based on traffic statistics as load or jitter can be collected by the switches. SDN is aimed at innovation of networks. In the networking world, it has found many uses including traffic engineering, mobility and wireless monitoring of network and networking in data-centre within several years from its beginning [2]. SDN is imagined as a great promise for the future internet. SDN [3, 4] is an emerging networking example that gives hope for changing the current network infrastructure limitations. First, it breaks the vertical integration by separating the control plane of networks from the underlying routers and switches that forward the data plane. Next, with the partition of the control and data planes, switches of the network become simple forwarding devices and the control logic is applied in a logically centralized controller, simplifying policy enforcement, network reconfiguration and evolution [5]. Figure A1 shows the simplified vision of this SDN architecture and its fundamental abstraction. It is important to emphasize that a logically centralized programmatic model does not postulate a physically centralized system [6]. In fact, the need to guarantee sufficient levels of performance, scalability, and reliability would prevent such a solution. Rather, SDN network production-level designs resort to physically distributed control logic [7, 8].

The control plane and the data plane separation can be studied by means of a programming interface. The state in the elements of data plane which is directly controlled by the controller is exercised via this well-defined Application Programming Interface (API), as represented in figure A1. [6] The strong coupling between control and data planes has made it hard to add new functionality to traditional networks, a fact illustrated in figure A2. [9, 10] Unlike the network devices the control plane is decoupled by SDN and becomes the network operating system or SDN controller.

3. SECURITY IN SOFTWARE DEFINED NETWORKING: CHALLENGES

[11] identifies that SDN faces a big challenge concerning remaining data centres. According to [12], integrating SDN in an enterprise needs an approximation of the needed number of controllers by defining the topology and these controllers localization. Moreover, a lack of know-how challenges can import risk of high security since the centralized software defined network controller can be very vulnerable compared to traditional networks [13]. [14] found out similar challenges when unskilled staff handled such architectures. They refer that protecting the operation of network need a migration and a well-considered roadmap to avoid having single failure points. [15] agreed that it is possible with SDN to meet challenges present in traditional networks, like intricate management. However, this technology has not yet matured so that current operators are faced with high difficulty instead of network architecture, easy management and easy building [16]. Another opinion states that SDN may currently be a well-established standard in some companies and industries but smearing this technology still needs a totally novel pool of know-how when it comes to updates of architecture from the operator’s side and to additional overhead meeting devices in present networks [17, 18, 19]. Specific examples of required know-how are the middle boxes deployment in choke points and traffic managing separation in networks [20].

3.1. Increasing demands

[21] recognizes numerous challenges about increasing demand when it comes to novel technologies. For example, the necessity of an appropriate and particular service for many traffic types such as conferencing through video or browsing through web in a very short time range and more requires improved utilization of resource for higher system performance and fast growth of SDN. [22] approved these points by saying that the user’s demand is not ever ending but instead is quickly growing which makes it essential to think about SDN. Particularly when it comes to quality of service or security issues, a new requirement for mobility, virtualization of server and cloud computing is required to meet the increasing demand. Hence, SDN still lacks and does not yet fulfil the demand because of whole network negative compromised resilience [23, 24]. According to [25], the quality of service topic is one of the core elements linked to the internet and has to handle rapid changing necessities and dynamic policies of distributed systems. All through the SDN field, providers now have a global view over the whole architecture. The existing equipment usage cannot meet the increasing

demand. The huge demand and device increase makes it necessary for the new technologies to invest and be a key enabler in growing new telecommunication infrastructure.

3.2. Implementation of SDN

In traditional networks one of the important challenges is the implementation of software defined networking as recognized. Existing research and industry solutions could resolve only some of these problems. [25] found out the problem of implementing novel technology without reinventing the entire architecture with its aspects and connected mechanisms. This view goes along with [26], which defined the long schedule of implementation as the biggest drawback [27]. The main features of the challenge consist of unexpected contact with other deployed networks, addition with legacy networks, which do not support the open flow protocol, errors of basic when emulating SDN beyond certain limits, updates of architecture and deep changes in inter-domain routing protocols, models of service and procedure of operation [28, 29]. [30] recognized, in addition to practical experiments, the economic restrictions of enterprises, as SDN needs a full "SDN-enabled" network deployment of switches and a serious re-engineering of the entire topology of network. [31, 32] Since SDN is very vulnerable, the adding deliberated flow tables can bypass the firewall.

4. CONSEQUENCE OF SDN

4.1. Special features of software defined networking

When compared to traditional networks, the SDN consists of numerous special features. The decoupling possibility of the forwarding plane from the data plane, leading to various abstraction layers is the most mentioned feature [33]. This can be defined [34] as a revolutionary change when comparing tight models of traditional networks [35]. This situation result in a data plane programmability such as interconnection of data centre and centralized control resolution due to a worldwide view over the entire network [36]. [37] complemented this by defining the protocol for open flow as a network visibility increase. The given API as a feature is also identified and delivered by SDN, to handle applications easily over the whole network [38]. Dynamic segmentation and utilization of demand-based network are moreover defined as SDN significant main features. A header informing additional optimization by using dynamic flows rather than static routing remarkably reduces the overhead on per byte transfer. A SDN-based architecture is reported for optimizing and a mechanism based on wireless LANs which provides the possibility of controlling the whole network remarkably with the advantages of an innovative and improved management is discussed.

4.2. Management of SDN

The management of an effective network is needed to handle methods series, tools and activities to finally confirm high quality for the user. Management of SDN includes set-up of network applications such as switches and controllers, installation, administering controllers and managing credentials between various entities of the SDN. [40] mentioned that SDN offers a global view over the whole topology resulting in an efficient management. The difficulty of cooperating management of SDN is high as it requires authentication. If it gets cooperated, the consequence on the network is severe. Threats of several securities can happen in the management. Because of this increasing demand there is a requirement for easy management through a discrete plane of common management. An application of unauthorized network, that comes from a third-party could contain a spiteful code. The constraint on applications to contact the controller server or the underlying managed network is very less in SDN. SDN is the biggest innovation in networking in the past two decades by uniting the network programmability principles and mechanizing. In distinguished to traditional networks, a SDN is not dependent on "dumb" devices which make decisions, but is based on a centralized controller which permits fast deployment and internationally based decisions.

4.3. Effect of software defined networking on economic factors

SDN offers great chances to raise efficiency and also to reduce cost and complexity [39]. Compared to traditional networks, [40] recognizes high possible network functions and dynamic allocation over nodes of network, but the testing process, experimenting and launching is still too time consuming and is not concordant with the needs of business. [41] indicated that at this point present networks are too exclusive and difficult to manage.

5. ANALYSIS OF IMPLEMENTATION ATTACKS AND INFLUENCE REVIEW

In attack analysis experiments, [40] classified those attacks for which there is no requirement of any kind of authentication to access an SDN system. From this viewpoint, the attack of data plane and the spoofing of control network are chosen. Figure A3 shows scenarios of overall attack for both cases. Analysis of these attacks revealed the impact on connection set-up latency and web clients requests on loss servers. With the growth of web-based businesses, the operators must authorize several service-level agreements (SLA) to their customers in web. Service availability and response-time are two of the critical metrics in any service-level agreements [42].

6. INTRA-SWITCH AND INTER-SWITCH COMMUNICATION

[42] Figure A3 shows that, web hosts are associated with switch 1 while adversaries are associated with both switches. Observed from figure A4 [42] that the outcome for this scenario is like the scenario of attack with less severity. An explanation for this is that as adversaries are distributed, flow tables and buffers of memory in web hosts side switch and the control connection of it with the controller are less occupied with flow requests as related to the previous cases of attack scenario [41].

SDN provides excessive chances to increase competence. Similarly it decreases costs and complexity. In addition, it has a facility for solving conflicts during installation for flow rules between several applications in a network. This limits fire wall rules and bypassing of a security application. It accounts for the rules of intra-table flow dependences in switches for detection of rule-conflicts. During adversarial attacks in an extension to open flow data plane has been discussed in order to decrease the interaction of control-data plane. This decreases the load on the controller for handling large flow requests. Architecture of the controller to protect the SDN from problems has been analysed in [43]. To limit the network applications access to the controller system and the managed network, a system of fine grained permission has been investigated for applications in [44]. Thus a framework for developing several applications of security over SDN is reviewed.

7. CONCLUSION

Software defined networking is seen as an evolution paradigm shift, but still faces numerous challenges and effects in the field of networking. The challenges and effects of the enclosed field offer an overall view of the reasons for slowing down, additional growth and feasibility when the technology is successfully integrated.

Furthermore, these reviewed papers mainly describe software defined networking on a very detailed platform in terms of mathematical and technological domains. However, the stable growth of users and necessities leave suppliers with the current network technologies usage in order to stay competitive and profitable. Thus the study has exposed the control and data plane separation proposals and their great benefits like virtual networks, dynamic deployment and economic factors. For further studies, attacks and services of network including VoIP, video streaming deployed in areal software defined networking tested for the analysis of attack can be considered. An overall risk evaluation for various threats can also be presented by evaluating their impacts on SDN managed networks. Apart from outlining the technical aspects, these benefits play a vital role in carrying out research. Software defined networking has a great future and ability to bring a network industry revolution.

REFERENCES

[1] Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K.Iyer and Zbigniew Kalbarczyk, Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges, Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, USA, 2015, pp. 61-68, http://dx.doi.org/10.1145/2732198.2732203.

[2] A.Akhunzada, E.Ahmed, A.Gani, M.Khan, M.Imran and S.Guizani, Securing Software Defined Networks:

Taxonomy, Requirements and Open Issues, IEEE Communications Magazine, Vol. 53, No. 4, 2015, pp. 36-44.

[3] Min Chen, Yongfeng Qian, Shiwen Mao, Wan Tang and Ximin Yang, Software-Defined Mobile Networks Security, Mobile Networks and Applications, 2016, pp. 1-15, http://dx.doi.org/10.1007/s11036-015-0665-5.

[4] Arnav Shivendu, Dependra Dhakal and Diwas Sharma, Emulation of Shortest Path Algorithm in Software Defined Networking Environment, International Journal of Computer Applications, Vol. 116, No. 1, 2015, pp. 47-49, http://dx.doi.org/10.5120/20304-2344.

[5] Junjie Xie, Deke Guo, Zhiyao Hu,Ting Qu and Pin Lv, Control Plane of Software Defined Networks: A Survey, Computer Communications, Vol. 67, 2015, pp. 1–10, http://dx.doi.org/10.1016/j.comcom.2015.06.004.

[6] Diego Kreutz, Fernando M.V.Ramos, Paulo Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky and Steve Uhlig, Software-Defined Networking: A Comprehensive Survey, 2014, pp. 1-61.

[7] Bhimshankar Mantur , Abhijeet Desai and K.S.Nagegowda, Centralized Control Signature-Based Firewall and Statistical-Based Network Intrusion Detection System (NIDS) in Software Defined Networks (SDN), Emerging Research in Computing, Information, Communication and Applications, Vol. 1, 2015, pp. 497-506, http://dx.doi.org/10.1007/978-81-322-2550-8_48.

[8] Peter Megyesi, Alessio Botta, Giuseppe Aceto, Antonio Pescape and Sandor Molnar, Available Bandwidth Measurement in Software Defined Networks, SAC, Pisa, Italy, 2016.

[9] Suyong Eum, Masahiro Jibiki, Masayuki Murata, Hitoshi Asaeda and Nozomu Nishinaga, A Design of an ICN Architecture within the Framework of SDN, Seventh International Conference on Ubiquitous and Future Networks, Sapporo, Japan, 2015, pp. 141-146.

[10] Nan Zhang and HeikkiHammainen, Cost Efficiency of SDN in LTE-based Mobile Networks: Case Finland, IEEE International Conference and Workshop on Networked Systems, Cottbus, Germany, 2015, pp. 1-5.

[11] Kashif Nisar KAS, Mohd Hanafi Ahmed Hijazi, Gang Chen and Abdolhossein Sarrafzadeh, A Review: Software Defined Networks Management, Proceedings of the Asia-Pacific Advanced Network, Vol. 39, 2015, http://dx.doi.org/10.7125/APAN.39.2.

[12] Haisheng Yu, Keqiu Li, Heng Qi, Wenxin Li and Xiaoyi Tao, Zebra: An East-West Control Framework for SDN Controllers, 44th IEEE International Conference on Parallel Processing, Beijing, China, 2015, pp. 610-618.

[13] E.Haleplidis, K.Pentikousis, S.Denazis, J.HadiSalim, D.Meyer and O. Koufopavlou, Software-Defined Network (SDN): Layers and Architecture Terminology, Internet Research Task Force (IRTF), RFC 7426, 2015, pp. 1-35.

[14] Peng Sun, Minlan Yu, Michael J. Freedman, Jennifer Rexford and David Walker, HONE: Joint Host-Network Traffic Management in Software-Defined Networks, Journal of Network and Systems Management, Vol. 23, No. 2, 2015, pp. 374- 399, http://dx.doi.org/10.1007/s10922-014-9321-9.

[15] Timothy Wood, K.K.Ramakrishnan, Jinho Hwang, Grace Liu and Wei Zhang, Toward a Software-Based Network: Integrating Software Defined Networking and Network Function Virtualization, IEEE Networks, Vol. 29, No. 3, 2015, pp. 36-41, http://dx.doi.org/10.1109/MNET.2015.7113223.

[16] Bing Wang, Yao Zheng, Wenjing Lou and Y.Thomas Hou, DDoS Attack Protection in the era of Cloud Computing and Software-Defined Networking, Computer Networks, Vol. 81, 2015, pp. 308-319,

http://dx.doi.org/10.1016/j.comnet.2015.02.026.

[17] Wei Wang, Yingjie Chen, Qian Zhang and Tao Jiang, A Software-Defined Wireless Networking Enabled Spectrum Management Architecture, IEEE Communications Magazine, Vol. 54, No. 1, 2016, pp. 33-39.

[18] Kottilingam Kottursamya, Gunasekaran Raja, Jayashree Padmanabhan and Vaishnavi Srinivasan, An Improved Database Synchronization Mechanism for Mobile Data using Software-Defined Networking Control, Computers & Electrical Engineering, 2016, http://dx.doi.org/10.1016/j.compeleceng.2016.01.019.

[19] Jian Li, Jae-HyoungYoo and James Won-Ki Hong, Dynamic Control Plane Management for Software-Defined Networks, 2016, http://dx.doi.org/10.1002/nem.1924.

[20] Daojing He, S.Chan and M.Guizani, Securing Software Defined Wireless Networks, IEEE Communications Magazine, Vol. 54, No. 1, 2016, pp. 20-25.

[21] Liwei Kuang, L.T.Yang, Xiaokang Wang, Puming Wang and Yaliang Zhao, A Tensor-Based Big Data Model for QoS Improvement in Software Defined Networks, IEEE Network, Vol. 30, No. 1, 2016, pp. 30-35.

[22] Peng Sun, Minlan Yu, Michael J. Freedman, Jennifer Rexford and David Walker, HONE: Joint Host-Network Traffic Management in Software-Defined Networks, Journal of Network and Systems Management, Vol. 23, No. 2, 2014, pp. 374-399, http://dx.doi.org/10.1007/s10922-014-9321-9.

[23] Adnan Akhunzada, Abdullah Gani, Nor Badrul Anuar, Ahmed Abdelaziz, Muhammad Khurram Khan, Amir Hayat and Samee U. Khan, Secure and Dependable Software Defined Networks, Journal of Network and Computer Applications, Vol. 61, 2016, pp. 199-221, http://dx.doi.org/10.1016/j.jnca.2015.11.012.

[24] Wendong Wang, Ye Tian , Xiangyang Gong , Qinglei Qi and Yannan Hu, Software Defined Autonomic QoS Model for Future Internet, Journal of Systems and Software, Vol. 110, 2015, pp. 122–135.

[25] Hui Yang, Jie Zhang, Yongli Zhao and Jianrui Han, SUDOI: Software Defined Networking for Ubiquitous Data Centre Optical Interconnection, IEEE Communications Magazine, Vol. 54, No. 2, pp. 86-95.

[26] Pascal Dauer, Rahamatullah Khondoker, Ronald Marx and Kpatcha Bayarou, Security Analysis of Software Defined Networking Applications for Monitoring and Measurement: Flow and Big Tap, The 10th International Conference on Future Internet Technologies, The K-Hotel, Seoul, Korea, 2015, pp. 51-56, http://dx.doi.org/10.1145/2775088.2775104.

[27] Anderson Santos da Silva, Paul Smith, Andreas Mauthe and Alberto Schaeffer-Filho, Resilience Support in Software-Defined Networking: A Survey, Computer Networks, Vol. 92, 2015, pp. 189–207, http://dx.doi.org/10.1016/j.comnet.2015.09.012.

[28] N.Cvijetic, A.Tanaka, P.Ji, K.Sethuraman, S.Murakami and Ting Wang, SDN and OpenFlow for Dynamic Flex-Grid Optical Access and Aggregation Networks, Journal of Lightwave Technology, Vol. 32, No. 4, 2014, pp. 864-870.

[29] C.Yin, T.C.Kuo, T.Y.Li, M.C.Chang and B.H.Liao, Mediating between OpenFlow and Legacy Transport Networks for Bandwidth On-Demand Services, 16th Asia-Pacific Network Operations and Management Symposium (APNOMS), Hsinchu, Taiwan, 2014, pp. 1-4.

[30] Julius Rückert , Jeremias Blendin and David Hausheer, Software-Defined Multicast for Over-the-Top and Overlay-based Live Streaming in ISP Networks, Journal of Network and Systems Management, Vol. 23, No. 2, 2015, pp. 280-308,

http://dx.doi.org/10.1007/s10922-014-9322-8.

[31] M. Moser and F. Jaramillo, Extending Software Defined Networking to End User Devices, The International Conference on Soft Computing and Software Engineering (SCSE), Computer Communication and Networks (ICCCN), Las Vegas, NV, 2015, pp. 1-8.

[32] Ferney A.Maldonado-Lopez, Eusebi Calle, Yezid Donoso, Detection and Prevention of Firewall-Rule Conflicts on Software-Defined Networking, 7th International Workshop on Reliable Networks Design and Modeling (RNDM), Munich, Germany, 2015, pp. 259 – 265.

[33] Madhusanka Liyanage, Ijaz Ahmed, Mika Ylianttila and Jesus Llorente Santos, Security for Future Software Defined Mobile Networks, 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, United Kingdom, 2015, pp. 1-9.

[34] Phillip Porras, Steven Cheung, Martin Fong, Keith Skinner, and Vinod Yegneswaran, Securing the Software-Defined Network Control Layer, Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, California, 2015, pp. 1-15, http://dx.doi.org/10.14722/ndss.2015.23222.

[35] A.Akhunzada, E.Ahmed, A.Gani, M.Khan, M.Imran and S.Guizani, Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues, Magazine in IEEE Communications, Vol. 53, No. 4, pp. 36-44, 2015.

[36] Brenton W.McMenamin , Chad J.Marsolek, Brianna K.Morseth, MacKenzie F.Speer, Philip C.Burton and E.Darcy Burgund, Conflicting Demands of Abstract and Specific Visual Object Processing Resolved by Frontoparietal Networks, Cognitive, Affective, & Behavioral Neuroscience, 2016, pp 1-14.

[37] M.Canini, P.Kuznetsov, D.Levin and S.Schmid, A Distributed and Robust SDN Control Plane for Transactional Network Updates, IEEE Conference on Computer Communications (INFOCOM), Kowloon, 2015, pp. 190-198.

[38] S.T.Yakasai and C.G.Guy, FlowIdentity: Software-Defined Network Access Control, IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, 2015, pp. 115-120.

[39] Yumi Oh and Sungwon Lee, Network Deployment and Implementation for Access Control with Open Source Based VNF, International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 105-107.

[40] Q.Yan, F.R.Yu, Q.Gong and J.Li, Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges, IEEE Communications Surveys & Tutorials, Vol. 18, No. 1, 2016, pp. 602-622.

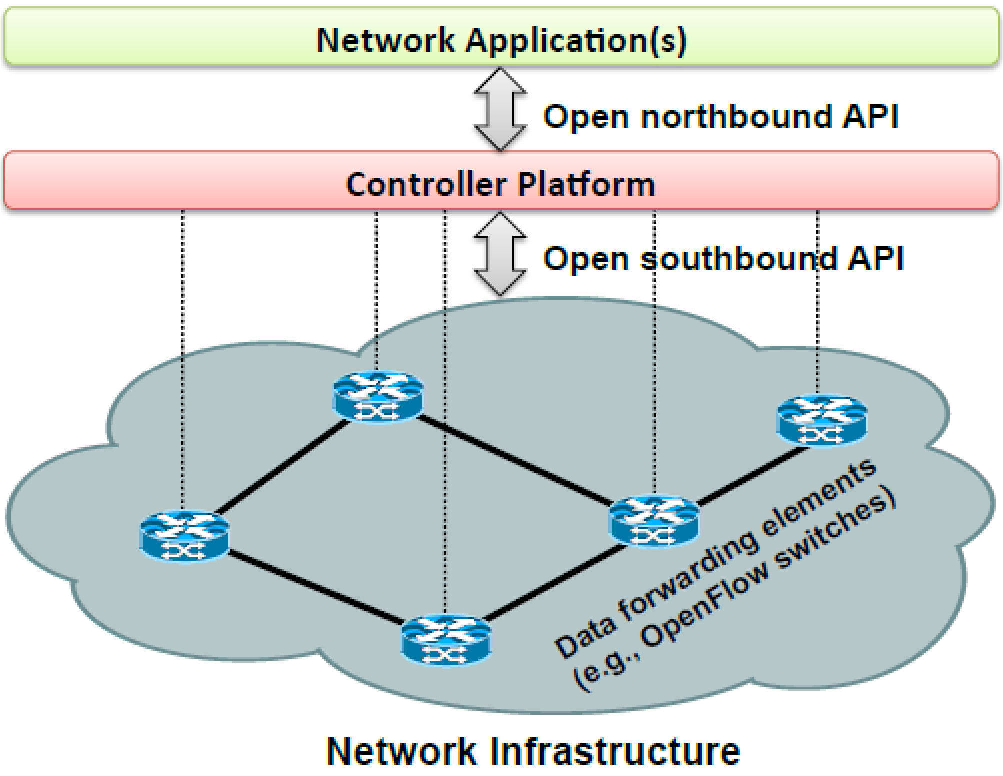
[41] H.T.Nguyen Tri and K. Kim, Assessing the Impact of Resource Attack in Software Defined Network, International Conference on Information Networking (ICOIN), Cambodia, 2015, pp. 420-425.

[42] Quamar Niyaz, Weiqing Sun and Mansoor Alam, Impact on SDN Powered Network Services under Adversarial Attacks, Procedia Computer Science, Vol. 62, 2015, pp. 228 – 235.

[43] Yufei Cheng, M.Moshfequr Rahman, S.Gangadhar, M.J.F.Alenazi and J.P.G.Sterbenz, Cross-layer Framework with Geodiverse Routing In Software-Defined Networking, 11th International Conference on Network and Service Management (CNSM), Barcelona, 2015, pp. 348-353.

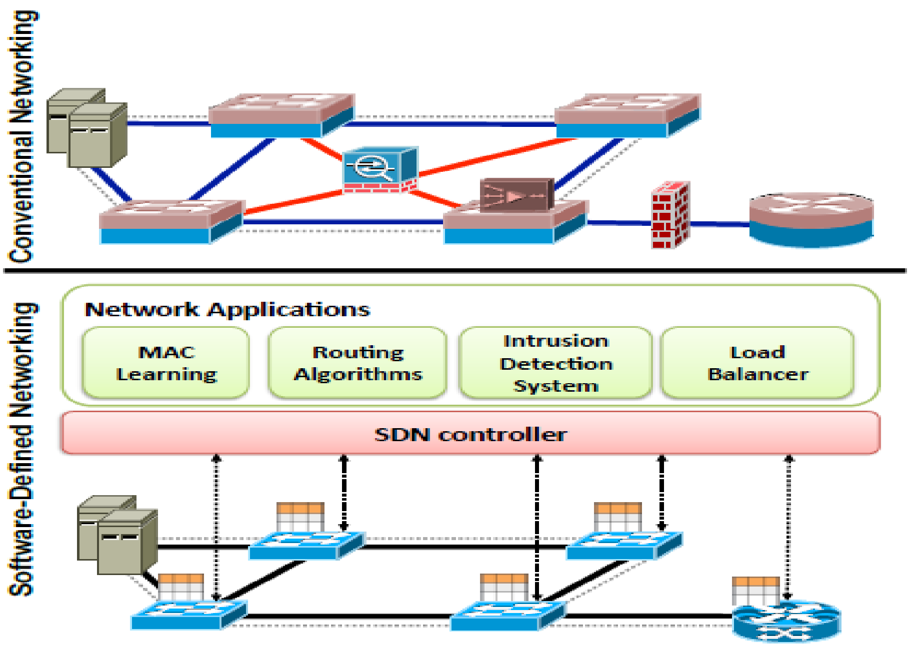
[44] A.Alba , C.Bolik and A.Corrao, Efficient and Agile Storage Management in Software Defined Environments, IBM Journal of Research and Development, Vol. 58, No. 2, pp. 1-12, 2014.

APPENDIX A



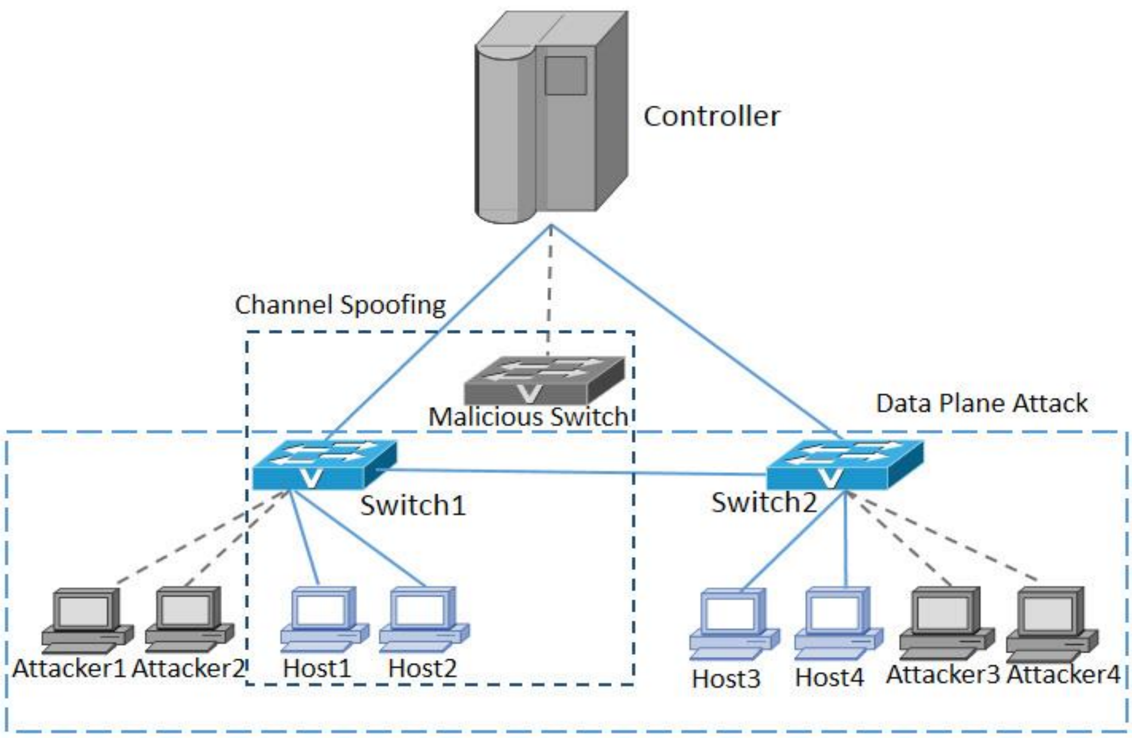
Adapted from [6]

Figure A1.Architecture of SDN and its concepts and building blocks



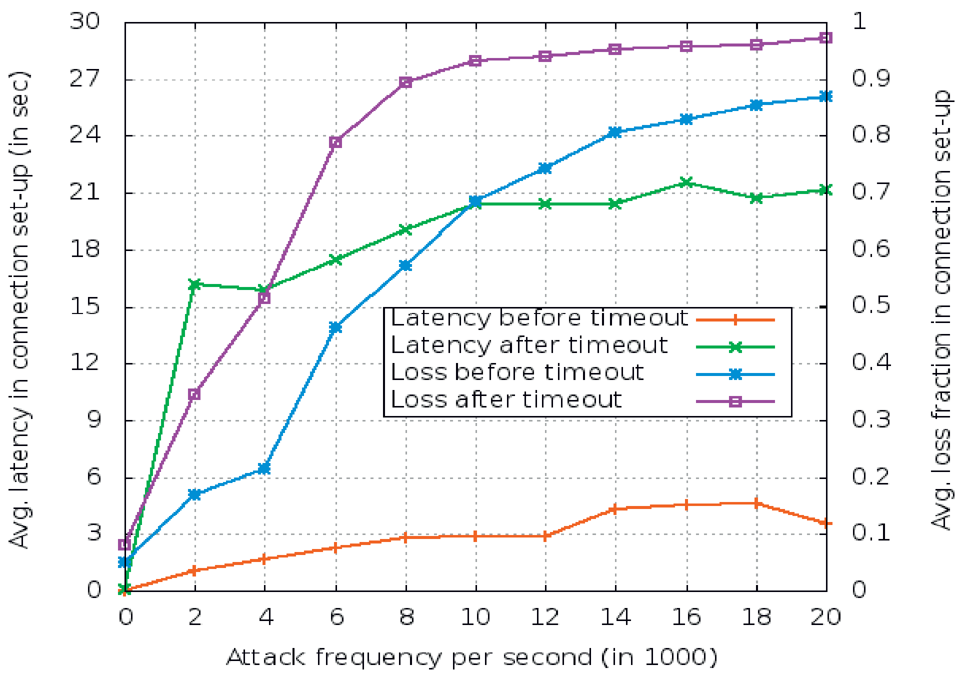
Adapted from [6]

Figure A2.Conventional networking Vs software networking



Adapted from [43]

Figure A3.Various attack scenarios implemented for web service performance analysis



Adapted from [43]

Figure A4.Connection set-up of average latency and loss average when web hosts exist on the similar network and adversaries located on dissimilar networks.