



Software Defined Networking: A Review with Existing Techniques

Hira Beenish, Muhammad Fahad, Usra Sami

College of Computing and Information Sciences, Karachi Institute of Economics and Technology

Department of Computer Science, Bahria University

hira@pafkiet.edu.pk, mfahad@pafkiet.edu.pk, Usrasami.bukc@bahria.edu.pk

Abstract— With the expansion of acute gadgets and rapid networks, the devices have expanded towards wide acknowledgments, that are the principle of widespread and low- manage networks. These devices can be managed remotely to play out the desired usefulness of network meanings. By using this concept SDN acts as a significant role in remote connections of these core devices. Because of separation of hardware & software it becomes easy to deploy on different devices in order to obtain software control then at the same time it is trying to manage these integrated techniques under the same ridge. This paper presents a comprehensive review of existing techniques used in software defined networking domain. This research article also presented some different constraints of software defined networks that is causing the efficient practice of software defined networking by comparing these constraints from different research articles.

Keywords: IP networks; Virtualization; Software defined networking; Computer networks; Security; Communication networks;

I. INTRODUCTION

We are living in an era of advanced technology, where everything vicissitudes day by day in other words our lives are becoming intellectual to become smarter than as we are now. Many gadgets are introduces and most of them need to connect with network because of that the network grows exponentially and to meet these necessities network devices becomes more complex [2-3], furthermore it's also very hard and time consuming for network administrator to configure on individual device due to even for very small change occurred in network like if any device is added or is removed so we have to reconfigure many routers and switches because of that little change and it may produce inconsistency and errors in any form human or devices [1].

SDN (Software Defined Network) is a concept of two different planes data and control, and move it into a centralized server through which all devices are connected so if any change occurred in network we just need to inform that server and it's not much harder it consumes very less time, so the all complexity of network management is shifted towards a software based controller (Centralized Server) and provide a fine underlying abstract infrastructure [4][5]. It allows controlling and managing the data plane and networking devices directly by central server [1].

Basically it's an architecture for remote networking. This approach allows then network administrator to manage, initialize, control and change network behavior dynamically through. [4]. SDN meant to address the static architecture i.e. traditional network which not supports the dynamic, as multiple hazards are there i.e. storage needs and scalable computing of modern computing environments. [2-5] It is a cost less solution because of centralized server and worked efficiently as it saves the time as well [3].

SDN has a great potential to change the way of network functioning but as it separates the data plane and control plane then now all control separates from the devices and

shifted to a central server. Because of separation of control plane from data plane [3].

Data plane fastly processed packets it looks at the packet header and then make a forwarding decision while the control plane puts the forwarding state there [5]. SDN seems like a revolutionary change in networking that's why it's growing at very fast pace and still there are many research challenges to be addressed and many network experts are working on it to make it more comfortable and proficient. A taxonomy of SDN architectural components with their implementations regarding of control plane & for the packet forwarding different flow are provided below in figure 1.

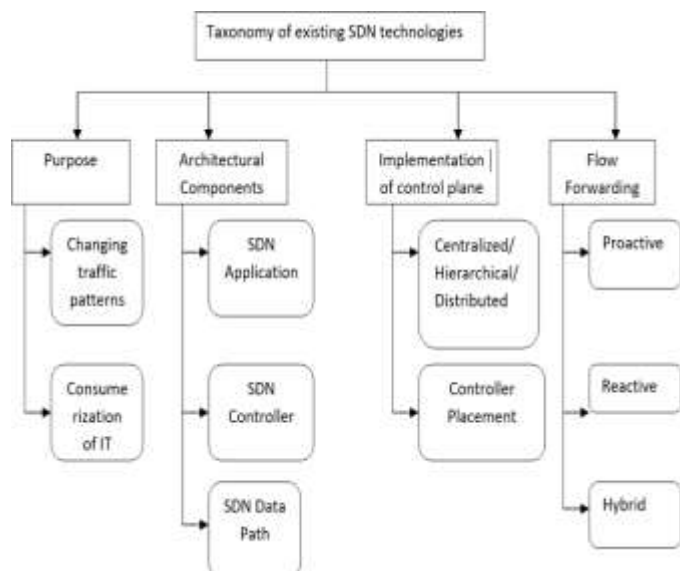


Figure 1. Taxonomy of Software Defined Network

The rest of the paper is organized as follows: Section II presents software defined networks architecture. Section III discusses the control planes with the help of application layer, control layer and infrastructure layer. After that Section IV discusses the open issues of in software defined networks in terms of security and security attacks. Later, Section V looks into Network virtualization. Finally, Section VI elaborates the scopes, limitations, future directions with concluding section.

II. SDN ARCHITECTURE

The architecture of SDN defines how a computing and networking system can build remotely [20]. In SDN Architecture there are three layers' data layer (data plane), controller layer and application layer. SDN is developed to enable programming control of networking in data-Path [10].

By decomposing control and data planes, SDN promises network management and flexibility towards innovation [1] A SDN controller framework is suggested that can allow a single application to run at both central and local controllers resulting in offload computation at local controllers [2]. For large scale networks, a simulation tool can be used to manage high traffic loads and policies [3]. As SDN is being evolved as an emerging technology, security is one important element and the security vulnerability assessment is an important and necessary process to undergo [4].

Data communication networks consists of end devices with the network infrastructure [3]. This is a shared infrastructure. It is quite difficult to deploy new versions of an existing protocol within the existing network and it's nearly impossible to deploy new protocol in existing infrastructure by deploying its architecture it becomes easier because of flexible architecture of SDN [5].

There are other architectures available for SDN which are technically different but the basic idea of SDN are same which is basic SDN principle of separation of control plane and data plane and they exchange information. Some of them are NFV& Open flow [7].

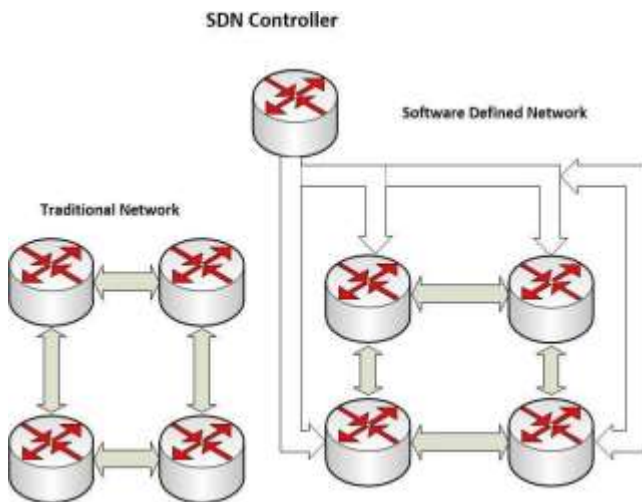


Figure 2. Comparison of SDN and traditional networking

Figure 2 differentiate the both forwarding actions of traditional networks with SDN. Basically SDN is the software that is connected to any hardware which is intended to forward or manage data. This is consisting of different kind of switches which we called SDN switches & traditional switches that are connected physically by different wires. Switches are the devices of which are used to forward packets that contain the rules which is used to formulate decision for packet forwarding. These some most common issues discussed in most of research papers and some papers possess some solutions for that but still not much effective.

III. DISTRIBUTED CONTROL PLANES

Distributed control planes are also good topic for research some researches must be made only on distributed control planes as basic idea of SDN is consist of control planes on it may give brighter image as SDN have now becomes the distributed system, are also it is in trend these days and already resolved many problems so it's a good clue for researchers to work on it [3]

SDN is divided in major three layers. Different kind of entities which are working in different layers can be anywhere in network. All the communication between them is compulsory and common.

A. Application Layer

Application layer is the top most layers where applications reside in the SDN architecture. These SDN applications need to communicate with the lower layer which is control layer. The communication is established using application programming interface (APIs) [19].

SDN applications can be of many types of network management or business applications, depending on each type, application layer can also collect information from the control layer for decision making and as well as to create an abstracted view of the whole network [2].

B. Control layer

The controlling of the entire network is done by control it is a brain of the software development network all records promote is occur in data layer but all the controlling is take place in control layer.

In Control Layer of the SDN architecture, SDN controller is logically responsible to receive instructions from the SDN application layer and further moves it forward to the networking devices.

SDN Controller can also receive information from the infrastructure layer and share it with the given SDN application acting as a middle man [1][9] Control Layer acts as a key requirement for the adoption of centralized control solutions in order to deploy a resilient, secure, dynamically configurable, adaptive, and virtualized infrastructure [18].

C. Infrastructure layer

The infrastructure layer contains networking hardware devices to control the movement of data. The APIs used to devise communications between SDN layers are referred as northbound and southbound interfaces [10].

IV. LITERATURE REVIEW OF OPEN ISSUES

There are many open issues in SDN as SDN growing fastly some issues already been resolved but some of most critical and complicated issues are still under discussion and many network experts are working to resolve these issues. Some of these are discussed below.

A. Security

Security is a vital element for SDN. For the deployment of SDN across different networks makers have to effort on security of SDN and makes it secure from attacks such as DOS attack malicious injections, spoofing attack etc. [10] [5][6][1] It is good area to work on but it's very complicated as well, researcher working on it for the enhancement of the security in sdn, authors proposed an approach in order to enhance the tables used in sdn based clouds in open flow architecture [26]. As discussed earlier it's a vital element that's mean wouldn't compromise on it in any case so they only way to make SDN able to use is overcome this issue which may attract people to use SDN because now it is the core part of networking [21-23].

B. Security Attacks

In the development of SDN, security is a big issue. There are many attacks that can relate to SDN attacks e.g. denial of service attack, distributed denial of service attack and flooding attacks. An attacker can affect the flood travel in small distance of time SDN enable network by using his own controllers. [24] Controller may be get caught and cannot differentiate between the usual passage and unusual passage.

Denial of service attacks are the major concern in distributed denial of service attacks. The new attack planes introduce from separation of data plane through control plane.

TABLE I. SECURITY ATTACKS ON SDN

Attacks	Security Property	Example
Tempering	Integrity	Data Falsifications
Spoofing	Authentication	IP & MAC spoofing
Denial of service	Availability	Numerous request to access server
Distributed DOS	Everywhere availability	Multiple request form all Borders
Repudiation	Non repudiation	Modification of source address

Above table I discusses the attacks and properties of the attacks with their examples. Security is the major concern of

any network. Above mentioned attacks are common attacks. By implementing security features we can save our network by implementing the solutions to make secure desired network. Integrity is related to data confidentiality in which same data is required for sender to receiver transmission. Authentication works for user ingenuity is used for the same data transferring as it comes from its original source. Data availability of intruder is another issue in these technologies, & if any data is available to the intruder they can generate the repudiation attacks on these devices. As it is a remote networking concept there are multiple technologies are available for the efficiently usage of these technologies discussed in [25].

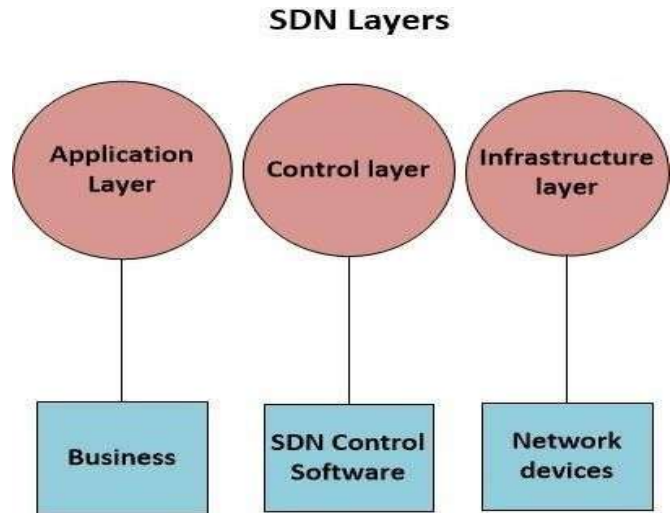


Figure 3. SDN Layers

Figure 3 shows the layers of Software defined network, Layer 1 is application layer which is based on the business application or interface of the application which connects with the second layer which is control layer, having functionality of network services which is connected with Layer 3 which is called infrastructure layer. In this layer different network devices are initiate.

TABLE II. CONCLUSION OF REFERENCED RESEARCH PAPERS SHOWING THE TARGETED RESEARCH GAP OF SDN

Paper	Security	Memory Efficiency	Software Reliability	Network Virtualization
[8]	✓	×	×	×
[9]	✓	×	✓	×
[10]	✓	✓	×	✓
[11]	×	×	×	✓
[12]	×	×	×	✓
[13]	×	×	✓	✓
[14]	×	✓	×	✓
[15]	✓	✓	×	×
[16]	✓	×	✓	×
[17]	✓	×	×	×

The above declared table II differentiate the different constraints used till now for software defined networking, a lot of work has been done in SDN. Implementations find errors in the form of memory utilization and remotely software reliability.

V. NETWORK VIRTUALIZATION

Network Virtualization is one of the hottest topic of networking as of today. The idea of network virtualization is to enable user to share resources and infrastructure remotely [4-6]. SDN has central control plane so that's why the idea of network virtualization is well achieved by SDN that why it's an open topic to research on and it pay back because it is in demand [10]. It not an easy task to work on because it is the integrations of many other constraints as well. A lot of more things are connected with it.

VI. CONCLUSION

In this paper aspects on SDN are thorough discoursed with the basic idea of that paradigm which is based on the separation of control and data plane are discussed with the requirements of SDN, remote networks grow at exponential rate and it's very difficult to manage it with the same technique i.e. hardware bindings with different software's.

There are several techniques available in sdn in order to enhance the traditional network proficiency, all of these techniques with their related issues are discussed in this paper. At the same time, we have presented challenges & open issues that are causes for the successively functioning of these techniques that needs to be addressed are also mentioned in this paper.

SDN is occupied in remote networks which will be remarkable achievement even some experts say that it's a biggest invention after smart phones.

REFERENCES

- [1] Rowshanrad, Shiva, Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, and Manijeh Keshtgary. "A survey on SDN, the future of networking." *Journal of Advanced Computer Science & Technology* 3, no. 2 (2014): 232-248.
- [2] D'Cruze, Hubert, Ping Wang, Raed Omar Sbeit, and Andrew Ray. "A Software-Defined Networking (SDN) Approach to Mitigating DDoS Attacks." In *Information Technology-New Generations*, pp. 141-145. Springer, Cham, 2018.
- [3] Akhunzada, Adnan, Ejaz Ahmed, Abdullah Gani, Muhammad Khurram Khan, Muhammad Imran, and Sghaier Guizani. "Securing software defined networks: taxonomy, requirements, and open issues." *IEEE Communications Magazine* 53, no. 4 (2015): 36-44.
- [4] Foerster, Klaus-Tycho, Stefan Schmid, and Stefano Vissicchio. "Survey of consistent software-defined network updates." *IEEE Communications Surveys & Tutorials* (2018).
- [5] Survey on Software-Defined Networking (IRACST - International Journal of Computer Science and Information Technology & Security (IJSITS), ISSN: 2249-9555 Vol.7, No.3, May-June 2017
- [6] Nunes, Bruno Astuto A., Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turetli. "A survey of software- defined networking: Past, present, and future of programmable networks." *IEEE Communications Surveys & Tutorials* 16, no. 3 (2014): 1617-1634.
- [7] Liao, Jianxin, Haifeng Sun, Jingyu Wang, Qi Qi, Kai Li, and Tonghong Li. "Density cluster based approach for controller placement problem in large-scale software defined networkings." *Computer Networks* 112 (2017): 24-35.
- [8] He, Ying, F. Richard Yu, Nan Zhao, Victor CM Leung, and Hongxi Yin. "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach." *IEEE Communications Magazine* 55, no. 12 (2017): 31-37.
- [9] Nunes, Bruno Astuto A., Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turetli. "A survey of software- defined networking: Past, present, and future of programmable networks." *IEEE Communications Surveys & Tutorials* 16, no. 3 (2014): 1617-1634.
- [10] Clad, Francois, Stefano Vissicchio, Pascal Méridol, Pierre Francois, and Jean-Jacques Pansiot. "Computing minimal update sequences for graceful router-wide reconfigurations." *IEEE/ACM Transactions on Networking (TON)* 23, no. 5 (2015): 1373-1386.
- [11] Davie, Bruce, Teemu Koponen, Justin Pettit, Ben Pfaff, Martin Casado, Natasha Gude, Amar Padmanabhan, Tim Petty, Kenneth Duda, and Anupam Chanda. "A database approach to sdn control plane design." *ACM SIGCOMM Computer Communication Review* 47, no. 1 (2017): 15-26.
- [12] Lee, Young, Maarten Visser, and T. Benjamin Mack-Crane. "Software defined networking (SDN) controller orchestration and network virtualization for data center interconnection." *U.S. Patent* 9,973,429, issued May 15, 2018.
- [13] Abdellatif, Ahmed Abdelaziz, Ejaz Ahmed, Ang Tang Fong, Abdullah Gani, and Muhammad Imran. "SDN-Based Load Balancing Service for Cloud Servers." *IEEE Communications Magazine* 56, no. 8 (2018): 106-111.
- [14] Hao, Zheng, Zhaowen Lin, and Ran Li. "A SDN/NFV Security Protection Architecture with a Function Composition Algorithm Based on Trie." In *Proceedings of the 2nd International Conference on Computer Science and Application Engineering*, p. 176. ACM, 2018.
- [15] Vizarreta, Petra, Kishor Trivedi, Bjarne Helvik, Poul Heegaard, Andreas Blenk, Wolfgang Kellerer, and Carmen Mas Machuca. "Assessing the Maturity of SDN Controllers with Software Reliability Growth Models." *IEEE Transactions on Network and Service Management* (2018).
- [16] Wrona, Konrad, Marek Amanowicz, Sebastian Szwaczek, and Krzysztof Gierlowski. "SDN testbed for validation of cross-layer data-centric security policies." In *Military Communications and Information Systems (ICMCIS), 2017 International Conference on*, pp. 1-6. IEEE, 2017.
- [17] Farhady, Hamid, HyunYong Lee, and Akihiro Nakao. "Software-defined networking: A survey." *Computer Networks* 81 (2015): 79-95.
- [18] Casellas, Ramon, Ricard Vilalta, Ricardo Martínez, and Raúl Muñoz. "Highly available SDN control of flexi-grid networks with network function virtualization-enabled replication." *Journal of Optical Communications and Networking* 9, no. 2 (2017): A207-A215.
- [19] Tatang, Dennis, Florian Quinkert, Joel Frank, Christian Röpke, and Thorsten Holz. "SDN-Guard: Protecting SDN controllers against SDN rootkits." In *Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017 IEEE Conference on*, pp. 297-302. IEEE, 2017.
- [20] Farhady, Hamid, HyunYong Lee, and Akihiro Nakao. "Software-defined networking: A survey." *Computer Networks* 81 (2015): 79-95.
- [21] Yadavalli, Krishna Teja, and Shatrunjay Rawat. "BotD: A scalable anomaly-based Bot Detection Architecture for securing web services." In *Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE Conference on*, pp. 69-73. IEEE, 2016.

- [22] Das, Tamal, Marcel Caria, Admela Jukan, and Marco Hoffmann. "Insights on SDN migration trajectory." In Communications (ICC), 2015 IEEE International Conference on, pp. 5348-5353. IEEE, 2015.
- [23] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378–403.
- [24] Hu, Z., Wang, M., Yan, X., Yin, Y., & Luo, Z. (2015, February). A comprehensive security architecture for SDN. In 2015 18th International Conference on Intelligence in Next Generation Networks (pp. 30-37). IEEE.
- [25] Beenish, H., & Fahad, M. (2019, January). 5G A review on existing technologies. In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.
- [26] Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, 10(5), 1985-1997.