Paper ID: 111

Multi-Controllers based subnet in SDN with BRS

4th International Conference on Information and Communication Technology for Competitive Strategy (ICTCS-2019), Udaipur, Rajasthan.

Introduction

- SDN is a novel solution to data communication and networking [1].
- Instead of configuration, network infrastructure, they are programmed to perform.
- SDN is a three-tier network architecture [2][3].
- The applications are at the highest level known as application.
- The middle level houses the controllers that manages the traffic [2][3].
- The lowest level consists of network devices that forms the infrastructure.
- Architecture of SDN is given in Fig 1 in the next slide.

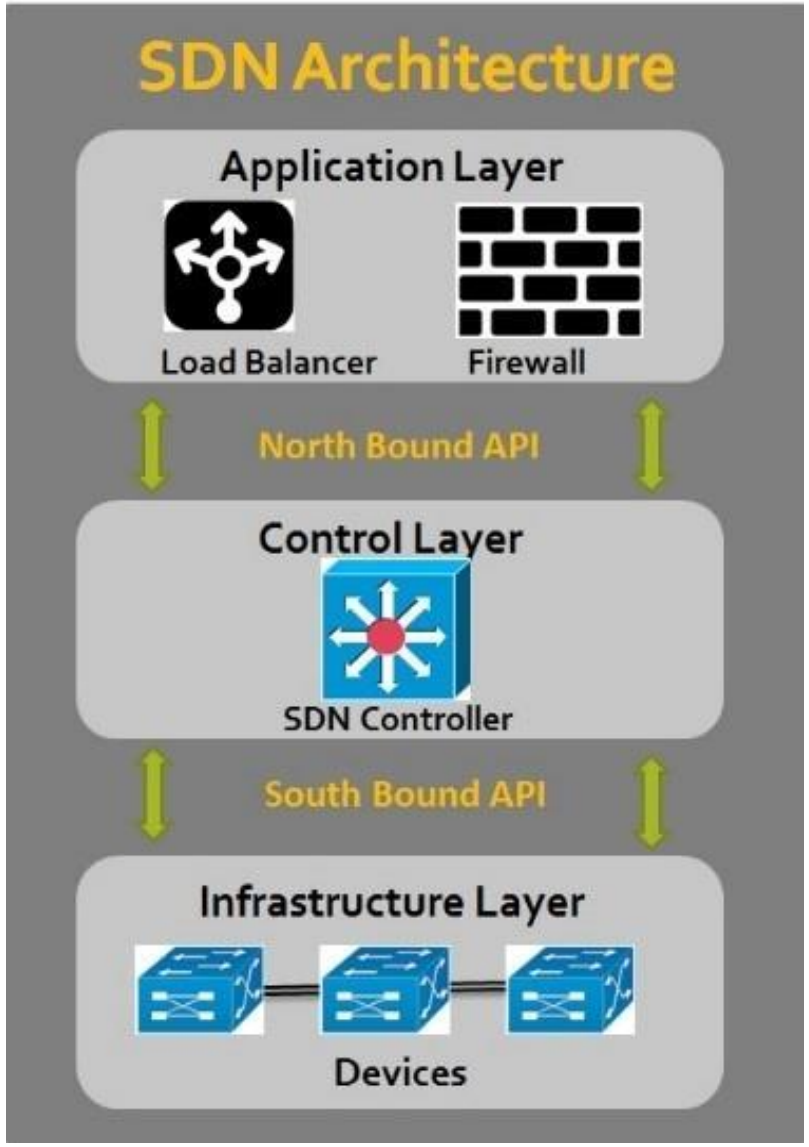

Fig.1 Showing the architecture of SDN

Priorities of SDN

- Controller management [4].
- Resource management [5].
- Security of SDN based networks.
- Attacks and sabotage on SDN based systems [6][7].

✓Unlike conventional network SDN has migrated the control plane to a centralized resource leaving data plane distributed.

✓Hence, Security of the SDN especially SDN controller is very important.

Security Issues related to SDN Controllers

SDN controllers are severely prone to attacks such as:

- Denial of Service (DOS),
- Replay attacks,
- Spoofing, etc.

SDN controllers are vulnerable because:

- Communication between controller and devices uses OpenFlow protocol [8].
- Managing traffic through south bound API increases vulnerability as these can be manipulated [9].
- Resource access is given higher priority compared to security [10].

Review Work

- Rossem et. al. deployed an elastic routing capability in an SDN / NFV enabled environment, but security is a major loophole in design [11].
- Boite et. al. proposed a stateful monitoring of SDN for DDOS attacks[12]. Authors did little work for controller-switch security and other types of controller attacks.
- Fan and Fernandez elaborated a TCP connection handover mechanism for hybrid honeypot systems which sacrifices to understand the attacks [13]. No mitigation proposal was given.

Review Work

- Dutta and Chatterjee proposed controller failure remedy using a Backup and Restoration System (BRS) [14]. A solution for both failure of standalone controller as well as controller placement problem in multiple controller environment. However, security issues are managed in a feeble manner.
- Dutta et. at. proposed a comprehensive solution with BRS in SDN [15]. Performance of the overall system is analyzed and an improvement with deployment is obtained in terms of throughput, packet drop, etc. However, unavailability of **High Available Redundant Controller** is a major limitation.

Research Gap & Problem Statement

- A limited work in the high-available controller environment using BRS with limited existence.
- Dutta et. at. proposed a comprehensive solution with single controller and BRS in SDN. However, High Available Redundant Controller is absent.

Hence a requirement of Redundancy is controller is the prime motivation for this research.

Proposed Technique

- Redundant or high-available controllers for individual subnet
- Each subnet will house two controllers one as master and the other as slave
- Slave is directly connected to the infrastructure and communicate using south bound API
- Slave connected to master using uplink.
- Fig 2 shows the deployment in multi subnet environment

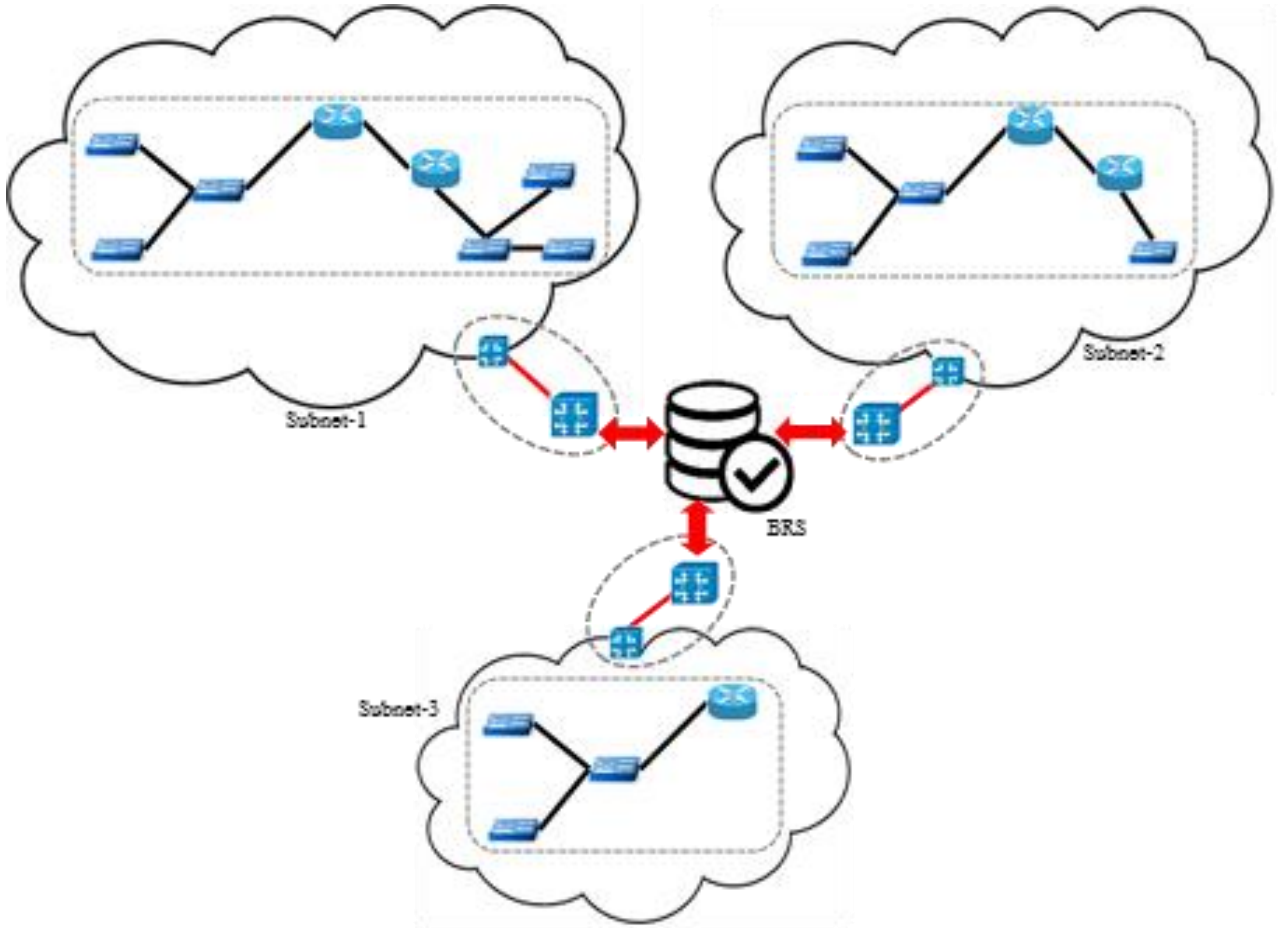

Fig. 2. Schematic diagram of multi-controller multi-subnet SDN with BRS.

Controllers in ordinary and extraordinary situation

- ✓Ordinary situation is when both controllers are working in specified roles
- ✓Extraordinary situation arises with occurrence of one of the following conditions:
  - The slave controller is down due to succumb to an attack or may breakdown due to hardware / software failure.
  - The master controller is down due to an attack or hardware / software failure.
  - Both master as well as the slave controller is down in a subnet due to attack or failure.

Measures in extraordinary situation

- The slave controller is down due to succumb to an attack or may breakdown due to hardware / software failure.

  Sol: The master will forward the traffic rules and manages the subnet

- The master controller is down due to an attack or hardware / software failure.

  Sol: The slave will continue to work without updating the current state of subnet to BRS. Hence, master controller of adjacent subnet is assigned to update BRS

- Both master as well as the slave controller is down in a subnet due to attack or failure.

  Sol: Master of an adjacent subnet will be assigned to forward traffic rules.

Results

Table 1. Benefits of proposed system with existing systems with and without BRS.

Sl. No.	Criteria	Existing system (without BRS)	Standalone system (with BRS)	Proposed system (with HA Controllers)	Remarks
1	**Backup support**	Within the Controller database	Centralized backup	Centralized backup and in Master controller	Better
2	**QoS**	Moderate	Better QoS	Better QoS	Better
3	**Performance**	Lack of Robustness	Moderate	Robust Architecture	More advance
4	**Reliability**	Less	Moderate	Highly reliable	More reliable
5	**Data loss**	May cause data loss	No loss in-case controller fails	No loss in case controllers fails	Reliable
6	**Maintenance**	Require instance maintenance	Have time for maintenance	Have sufficient time for maintenance	Spare time available
7	**Cost**	Less costly	Cost for BRS	Cost for BRS and HA controllers	One-time high expenses
8	**Efficiency**	Resource not available in case of failure	Moderately available	Highly available	More efficient
9	**Adaptability**	Not fault adaptive	Fault adaptive	Fault tolerant	Better adaptive
10	**Security**	Less secured	Moderately Secured	Proactive security measures	More secured

Conclusion and Future Scope

- A system proposed with HA controller arranged in master-slave configuration along-with a BRS to improve the overall reliability
- It is obvious to incur more cost for multiple controllers for individual subnet with BRS.
- This additional cost may be justified with higher reliability, better management of controllers in ordinary and extraordinary situation.
- In future, the authors will try to address the security measures taken for communication between the master and slave controllers.

Acknowledgement

The authors thank the members of faculty and staff of the Department of Computer Science and Engineering at NITTTR, Kolkata and University of Kalyani, Kalyani as well as DST PURSE, University of Kalyani, Kalyani for their immense support and assistance in carrying out this research work.

References

1. Kreutz, D., Ramos, F., EstevesVerissimo, P., Esteve Rothenberg, C., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE 103, 14 –76 (2015).
2. Nishtha, Sood, M.: A survey on issues of concern in software defined networks. In: 2015 Third International Conference on Image Information Processing (ICIIP), pp 295–300 (2015).
3. Othmane B., Mamoun, M.B., Benaini R.: An Overview on SDN Architectures with Multiple Controllers. Journal of Computer Networks and Communications 2016, 1-8, (2016), http://dx.doi.org/10.1155/2016/9396525, last accessed 2019/06/21.
4. Berde, P., et al.: ONOS. In: Proceedings of the Third Workshop on Hot Topics in Software Defined Networking - HotSDN 2014, pp 1–6 (2014).
5. Dixit, A., Hao, F., Mukherjee, S., Lakshman, T., Kompella, R.: Towards an elastic distributed SDN controller. In: ACM SIGCOMM Computer Communication Review, vol. 43. pp 7–12 (2013).
6. UlHuque, M., Si, W., Jourjon, G., Gramoli, V.: Large-scale dynamic controller placement. IEEE Trans. Netw. Serv. Manag. 14, 63 –76 (2017).
7. Xia, W.,Wen, W., Foh, C. H. Niyato, D., Xie, H. A Survey on Software-Defined Networking. IEEE Communication Surveys & Tutorials 17(1), 27-51 (2015).
8. Zhang, H., Cai, Z., Lui, Q., Xiao, Q., Li, Y., Cheang, C. F.: A Survey on Security-Aware Measurement in SDN. Journal of Security and Communication Networks, Wiley-Hindawi, (2018) pp 1-14.

9. Cabaj, K, Wytrebowicz, J., Kuklinski, S., Radziszewski, P., Truong Dinh, K.: SDN Architecture Impact on Network Security. Federated Conference on Computer Science and Information Systems, Warsaw, Poland, September, (2014). pp 143-148.

10. Sezer, S., Scott-Hayward, S., Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M., rao, N.: Are We Ready for SDN? Implementation Challenges for Software-Defined Networks. IEEE Communication Magazine, July (2013). pp 36-43.

11. Rossem, S.V., Tavernier, W., Sonkoly, B., Colle, D., Czentye, J., Pickavet, M., Demeester, P.: Deploying elastic routing capability in an SDN/NFV-enabled environment. In: IEEE Conference on Network Function Virtualization and Software Defined Networks, Demo Track, pp 22-24, IEEE. (2015).

12. Boite, J, Nardin, P.A., Rebecchi F., Bouet, M., Conan V. Statesec: Stateful monitoring for DDoS protection in software defined networks. In: 2017 IEEE Conference on Network Softwarization (NetSoft) IEEE. Bologna Italy (2017).

13. Fan, W., Fernández, D. A novel SDN based stealthy TCP connection handover mechanism for hybrid honeypot systems. In: 2017 IEEE Conference on Network Softwarization (NetSoft). IEEE. Bologna Italy (2017).

14. Dutta, P., Chatterjee, R. A Novel Solution for Controller Based Software Defined Network (SDN). In: J. K. Mandal and D. Sinha (eds.): 52nd Annual Convention Computer Society of India (CSI 2017), CCIS 836, pp. 90–98, Springer Nature. (2018).

15. Dutta, P., Chatterjee, R., Mandal, J. K. An approach for deployment of BRS in software-defined network. Innovations in Systems and Software Engineering, Springer-Nature Published Online: 02 May 2019.

Thanks and Question if any