Design problems towards reliable SDN Networks

Carmen Mas Machuca[1], Petra Vizarreta[1], Raphael Durner[1], Dorabella Santos[2], Amaro de Sousa[3]
[1]*Chair of Communication Networks, Technical University of Munich, Germany*
e-mail {cmas, petra.stojsavljevic, r.durner}@tum.de
[2] *Institute of Telecommunications, Portugal*
e-mail dorabella@av.it.pt
[3]*Institute of Telecommunications, University of Aveiro, Portugal*
e-mail asou@ua.pt

Abstract: Software Defined Networking offers many advantages such as cost reduction, higher flexibility and network programmability by decoupling the control from the data plane. In order to also increase reliability, several design problems are presented.
OCIS codes: (060.4257) Networks, network survivability; (060.4250) Networks

Software Defined Networking (SDN) architecture is based on a logically centralized network control, which is separated from the data plane. SDN promises several advantages such as cost reduction, fast provisioning, scalability and load balancing. However, reliability has to be considered in order to guarantee the expected network behavior in case of single and/or multiple failures or attack occurrence. For the remaining of this summary, the term failures will also cover attacks, since they can be considered as targeted and/or intentional failures.

The basic SDN architecture [1] consists of three planes as depicted in Fig. 1: (i) the application plane (at the top), (ii) the controller plane (in the middle) and (iii) the data plane (at the bottom) which corresponds to the infrastructure layer (i.e., the interconnected set of network elements able to forward and process data with minimum management and control functionalities). The control layer consists of a set of one or more SDN controllers which is responsible to translate the application requirements into control actions towards the network elements and to inform the applications about any relevant notify from the data plane. The architecture also includes a Management plane in parallel to the three previous planes to provide all the required management functions (e.g., configuring the SDN controller assigned to each network element, configure controller policies).

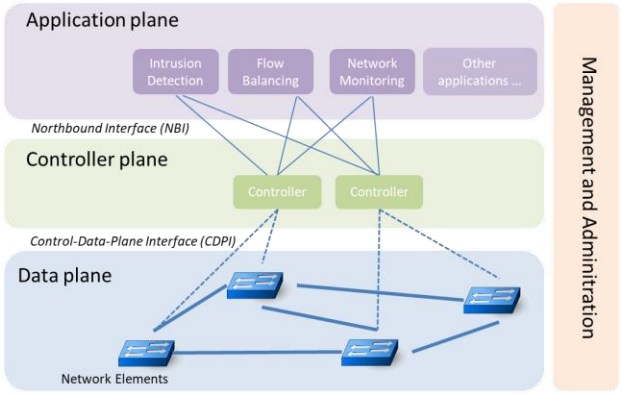

Fig. 1 SDN Architecture [1]: This summary focuses on the controller and data planes as well as on the control flows between them

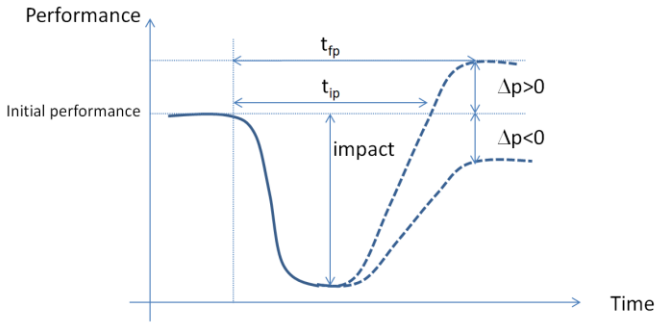

Fig. 2 Resilient profile parameters

In order to increase the reliability of the network, the potential failures should be identified and modelled in terms of occurrence, impact and dependency with other failures. The failures addressed in this summary cover failures that can occur (i) at the data plane, (ii) at the controller plane, and/or (iii) at the control flows between controller and network elements.

- Data Plane: Failures at the network infrastructure such as link failures (e.g., cable cut) and network element failures (e.g., card failure, power cut) may occur interrupting any data flow using that failed component. Existing mechanisms such as protecting data flows with disjoint paths or precomputing potential restoration paths for configured data flows can be used. Protecting data flows is a proactive recovery solution useful mainly in case single failure occurs [2, 3]. However, if multiple failures occur, reactive recovery solutions aiming at restoring the interrupted flows are most suitable since it allows finding restoration paths (if the network is still connected) but it is executed at the control plane [2].

- Controller Plane consists of one or several controllers. In order to increase scalability and avoid having a single point of failure, several controllers can be distributed throughout the network. Different architectures have been proposed: flat architectures (all controllers at the same level, e.g., primary/back-up solution [4,5]), or hierarchical architectures [6].

  A key aspect in the design of reliable SDN networks is the controller placement problem, i.e., how many controllers to use and which location to deploy for each of them. A standard way to reach controller plane reliability is to use primary/back-up solutions. Then, taking into account the back-up features of existing architectures and the network topology of the data plane, the reliability of the SDN network can be significantly enhanced, as in [7] where each switch is controlled by a pair of primary/back-up controllers and the data plane provides a pair of disjoint control paths (one for each controller). The way back-up is provided can also have an impact on the reliability gains. The basic approach is to have a back-up controller for each primary controller. Nevertheless, more flexible approaches can consider that a controller can provide back-up to multiple primary controllers and, more generally, controllers can be both primary and back-up controllers. Such additional flexibility imposes new challenges in the SDN architectures (they become more complex to manage) but can be used to further enhance the network reliability, as in [8] where any controller can act as a primary and/or back-up controller enabling optimal reliability for a given data plane topology with small control plane performance penalties.

  Controllers may have software failures (e.g., due to bugs or misconfigurations) or hardware failures (e.g., due to equipment power cut or crashed disk). Using back-up controllers may reduce the failure impact in some failure scenarios [7,8] but not for failures/attacks due to bugs and vulnerabilities, since they may appear in all controllers. Hence, special attention to software failure reliability has been done by modeling and analyzing different SDN controllers [9]. Furthermore, attacks addressing the software nature of controllers such as syntactic or semantics (e.g., Denial of Service) attacks have also been considered [10,11].
- The communication flow between network elements and the assigned controller is referred as control flow. These control communications can be implemented as out-of-band or in-band control. The former requires separate communication channels for control and data planes, and hence, some solutions propose using the data plane if the control channel fails. The in-band architecture allows both planes to use the same communication channel and hence, can fail at the same time [7, 8, 12].

For any potential failure or attack, the resilience profile gives an overview of its impact [13]. This profile shows how the performance varies in the event of a failure or attack. As depicted in Fig. 2, the resilience profile is characterized by the impact of the failure/attack measured by the decrease of performance, the time to restore the initial performance (t_{ip}), the time to reach the final performance (t_{fp}), and the difference between the final and the initial performance Δp (positive if the system outperforms or negative if the system underperforms).

Based on the different solutions addressing different failures/attack problems, design guidelines towards a reliable SDN network will be presented.

References

[1] ONF Technical Report TR-502 “SDN architecture” (June 2014)

[2] A. Xie et al. “Designing a Disaster-resilient Network with Software Defined Networking” *IEEE 22nd International Symposium of Quality of Service (IWQoS)*, Hong Kong, (2014) pp. 135-140.

[3] A. Sgambelluri, et al., "OpenFlow-based segment protection in Ethernet networks," IEEE/OSA Journal of Optical Communications and Networking, vol. 5, issue 9, pp. 1066-1075, 2013.

[4] A. Dixit, et al. “Towards an elastic distributed SDN controller,” in Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN '13) ACM, Hong Kong, 2013

[5] X. Chen, et al. “Leveraging master-slave OpenFlow controller arrangement to improve control plane resiliency in SD-EONs” OPTICS EXPRESS, Vol 23, No. 6, March 2015

[6] S. H. Yeganeh and Y. Ganjali, “Kandoo: a framework for efficient and scalable offloading of control applications,” in HotSDN 2012

[7] P. Vizarreta-Stojsavljevic, C. Mas Machuca, W. Kellerer “Controller Placement Strategies for a Resilient SDN Control Plane”. 8th International Workshop on Reliable Networks Design and Modeling (RNDM), 2016

[8] D. Santos, A. de Sousa, C. Mas Machuca “Robust SDN Controller Placement to Malicious Attacks” IEEE Int’l Conf. on Design of Reliable Communication Networks (DRCN), 2018

[9] P. Vizarreta-Stojsavljevic, K. Trivedi, B. Helvik, P. Heegaard, W. Kellerer, C. Mas Machuca “An Empirical Study of Software Reliability in SDN Controllers”. 13th International Conference on Network and Service Management (CNSM), 2017

[10] R. Durner, C. Lorenz, M. Wiedemann, W. Kellerer “Detecting and Mitigating Denial of Service Attacks against the Data Plane in Software Defined Networks” IEEE Netsoft 2017

[11] D. Kreutz, F. Ramos, P. Verissimo, “Towards Secure and Dependable Software-defined Networks“ Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN) 2013

[12] S. Sachin, et al. "Fast failure recovery for in-band OpenFlow networks," IEEE Int’l Conf. on Design of Reliable Communication Networks (DRCN), 2013

[13] E. Massaro, A. Ganin, N. Perra, and I. Linkov “Resilience management during large-scale epidemic outbreaks” Scientific Reports 8(1) DOI10.1038/s41598-018-19706-2 October 2017