Enhancing Availability on IP Network using Active-Active Replication of SDN controllers

Aye Myat Myat Paing
University of Computer Studies (Thaton)
paing.ayemyat@gmail.com

Abstract

The exponential growth of mobile devices and server virtualization and cloud computing technologies are the key computing trends which need new networking architecture. Nowadays, Software Defined Networks (SDN) has established a lot of attention as a new technology which provides more flexibility than conventional network which has programmability, configurability and manageability from its unique character of centralized software control. Therefore, this paper focus on enhance system availability using SDN concept for IP network. Since the controller is centralized, it will be a potential single point of attack and failure. The SDN controller affects the overall availability of SDN. To overcome the single point of failure, SDN controller is replicated with active-active replication. The SDN controller can suffer software failure as well as hardware failure. To prevent system failures caused by software, software rejuvenation can be applied. The impact of failure on SDN controllers is illustrated the analytic model and evaluate with the steady-state system availability through the use of numerical analysis.

Keywords: Software Defined Networking, Availability, Proactive software rejuvenation.

1. Introduction

The lack of flexibility and programmability of legacy network architecture has been the concern of many networking enthusiast over the years. The necessity to overcome these lapses in today's network has been the focus of many industry and academic research efforts [3]. Consequent upon these remarkable contributions is the requirement to deliberately isolate the functionality of the data plane from that of the control plane. The current standard, in which the data forwarding functions and the control functions are built into a single hardware, is the reason for and the basis of the lack of flexibility and programmability of the current network structure. The argument has been made and reasonably so, that if the data and control functions are decoupled and isolated from the single plane. During recent year, SDN is the decoupling of the data plane from the control plane. In addition, the control plane is logically centralized in a software defined controller (network brain), while the data plane is composed of network devices (network arms) [4].

SDN centralized control, logically centralized SDN controllers are potentially focused to a different set of risks and threats compared to traditional IP network architectures. The availability of SDN controller is more important issue for the overall system availability. The SDN controller can face from hardware and software failure. In order to solve the software failure, proactive software rejuvenation is applied. When SDN controller suffers hardware failure, we will switch to another replicated active SDN controller in order to reduce the downtime. Furthermore, with two controllers functioning as active production servers, you can make better use of resources by balancing workloads.

In this work, to avoid the operation overhead in the traditional IP network, we take the advantage of new networking technology of SDN and offer a proactive software rejuvenation solution for software failure for SDN controllers. The organization of this paper is as follows. In section 2 we discuss the related work. The system architecture for active-active replication of SDN controller is presented in section 3. The proposed model for enhancing system availability follows in section 4. Finally we conclude our paper in section 5.

2. Related Work

In this section selected publications are reviewed which related to our work. Sousa et.al [8] proposed a complementary approach that enhances proactive recovery with additional reactive mechanisms giving correct replicas the capability of recovering other replicas that are detected or suspected of being compromised. One key feature of their proactive-reactive recovery approach is that, despite recoveries, it guarantees the availability of a minimum number of system replicas necessary to sustain correct operation of the system. In the paper [1], the authors proposed a unified server-network resource management for such converged Information and Communication Technology (ICT) environments. They presented a SDN-based orchestration framework for live Virtual Machine (VM) management that exploits temporal network information to migrated VMs and minimize the network-wide communication cost of the resulting traffic dynamics.

The researchers commenced with a listing of identifiable security threats and breaches of Software Defined Networking in paper [2]. Then, it made an analysis of their previously solution to identifiable security issues of SDN. They ventured further into the horizon of the unknown to predict and identify new security breaches and threats, as well as areas of inherent weakness in the overall SDN architecture and infrastructure. Possible solutions to the identified issues are proffered and analyzed by the paper. In view of the limitations of this research, they prescribed possible positions for future researchers to adopt, in order to shed more light to the pertinent security issues of SDN. The author Rout et. al presented how SDN has taken the major role in current situations in [6]. SDN separates the control plane and data plane to make the routing more versatile. They modeled the packet-in message processing of SDN controller as the queuing systems M/M/1. The researchers [11] considered dynamic controller assignment sp as to minimize the average response time of the control plane.

In paper [5], the authors proposed a two-level modeling approach that is used to evaluate the availability of the SDN number, homing and location of SDN controllers. Their results showed how network operators can use the approach to find the optimal cost implied by the connectivity of the SDN control platform by keeping high levels of availability. Thein et. al presented that virtual machine based software rejuvenation (VMSR) model is developed using stochastic modeling. But it only captured VM level software fault behavior due to software failure [9].

3. System Architecture for Active-Active Replication of SDN controllers in IP network

This system consists of virtualized cluster severs with IP network using SDN concept. There are two SDN controllers which are setting up with active-active replication. System architecture is shown in Figure 1. The system architecture is based on SDN concept of IP network which is a communication *network* that uses *Internet Protocol* (*IP*) to send and receive messages between one or more computers. In this architecture, there are two SDN controllers in control plane and router and virtualized servers are in data plane.

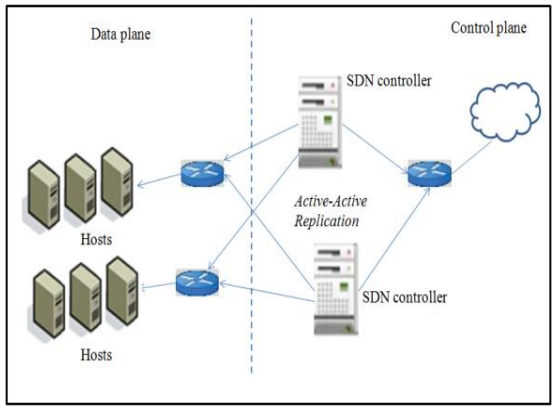

Figure 1. System Architecture for Active-Active Replication for SDN controller

In SDN environment, the controller being the central authority taking the routing decision of the packet. The router receives the packet from the source and sends it to the controller for processing. Therefore, SDN controller is one of the important factors of enhancing overall system availability.

Consequently, the active-active replication is applied in SDN controller in order to get minimize downtime for this IP network. These two SDN controllers are synchronized and can be used for resources by balancing workload. One of the controllers fail due to hardware fault, the other active controller can be switched with less significances of system downtime. When the SDN controller suffers software failure, the proactive rejuvenation is applied.

4. Proposed Model for Enhancing System Availability

In this section, we present state diagram for proactive software rejuvenation on active-active replication of SDN controllers as shown in Figure 2. If the active SDN controller is about to be switched cause of hardware failure, it is switched to another active replication controller and then will be started for the new requests and sessions. It can return back to the active controller after the completion repair control hardware. For Software failure, the SDN controller will be rejuvenated and switched to another active replica controller.

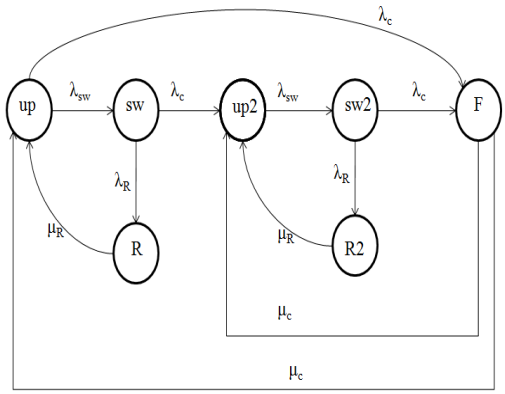

Figure 2. State Diagram of System Availability Model

The above state diagram has seven states in total. Each state has probability of being in its own state. The states are given as per SDN controller. In active SDN controller, there are three states like Up state (up), Software failure state (sw) and Rejuvenation state (R). We use Markov chain formulation for analyzing the above states. Active SDN controller provides the services in the Up state (up). If controller is software failure then it moves to the Software failure state (sw) through rate λ_{sw}.

At that time the active controller is move to Up states of another active replication controller through λ_c. From SW state, moves to the proactive software rejuvenation state (R) with rate λ_R. We try to consider almost all possibilities of going down when there is no active controller in SDN network. From the system outage, all SDN controllers can be repaired through the rate of μ_R.

Table 1. Steady-state probabilities

Symbol	Meaning
P_{up}	Probability of active SDN controller Up state
P_{sw}	Probability of Software Failure state in active SDN controller
P_R	Probability of Proactive Software Rejuvenation state in active SDN controller
P_{up2}	Probability of active replica SDN controller Up state
P_{sw2}	Probability of Software Failure state in active replica SDN controller
P_{R2}	Probability of Proactive Software Rejuvenation state in active replica SDN controller
P_F	Probability of being in Failure state

The conservation equation of Figure 2 is obtained by summing the probabilities of all states in the system and the sum of the equation is 1. The meaning of steady state probabilities is shown in Table 1.

$$P_{up} + P_{sw} + P_R + P_{up2} + P_{sw2} + P_{R2} + P_F = 1 \quad (1)$$

We acquire the closed-form solution for the system.

$$P_R = \frac{\lambda_R}{\mu_R} P_{sw} \quad (2)$$

$$P_{up} = \frac{\lambda_c + \lambda_R}{\lambda_{sw}} P_{sw} \quad (3)$$

$$P_F = \frac{1}{\mu_c} B P_{sw} \quad (4)$$

$$P_{up2} = \frac{1}{\lambda_{sw}} A P_{sw} \quad (5)$$

$$P_{sw2} = C P_{sw} \quad (6)$$

$$P_{R2} = \frac{\lambda_R}{\mu_R} C P_{sw} \quad (7)$$

$$P_{sw} = \left[1 + \frac{\lambda_R}{\mu_R} + \frac{\lambda_c + \lambda_R}{\lambda_{sw}} + \frac{1}{\mu_c} B + \frac{1}{\lambda_{sw}} A + C + \frac{\lambda_R}{\mu_R} C\right]^{-1} \quad (8)$$

Where $A = \left[\lambda_c + (\lambda_{sw} + \lambda_c)\frac{\lambda_c + \lambda_R}{\lambda_{sw}}\right]$

$$B = (\lambda_{sw} + \lambda_c)\frac{\lambda_c + \lambda_R}{\lambda_{sw}} - \lambda_R$$

$$C = \frac{1}{\lambda_c + \frac{\lambda_R{}^2}{\mu_R}} A$$

4.1 Availability and Downtime Analysis

Availability is a probability of a SDN concept with IP network which provides the services in a given instant time. In this model, we focus on SDN controller services. When both controllers fail in active-active replication of SDN network, the system will down. Markov chain will be classified as up states or down states. The system is not available in the failure state (F). Downtime is evaluated in an interval of T time units.

The system availability in the steady-state and Downtime are defined as follows:

Availability = 1-Unavailability (9)

Availability = 1-P_F (10)

Downtime (T) = T* P_F (11)

In order to examine the behavior of the system studied, we perform numerical analysis using the system-parameters [4, 7] as shown in Table 2.

Table 2. Parameters values and description

Parameter	Description	Values
$1/\lambda_c$	Mean time to controller hardware failure	6 months
$1/\lambda_{sw}$	Mean time to Software failure	1 week
$1/\lambda_R$	Mean time to Software repair	3mins
$1/\mu_R$	Proactive Software Rejuvenation Time	5 mins
$1/\mu_c$	Controller Hardware Repair Time	12hrs
T	Unit Time Interval	24*30*12 days

The influence of SDN controller hardware repair time along with different controller hardware failure time on availability is shown in Figure 3. The SDN controller hardware repair times are assumed 6 hours and 12 hours. The lower mean time to SDN controller hardware repair time, the higher availability of our system model can be achieved.

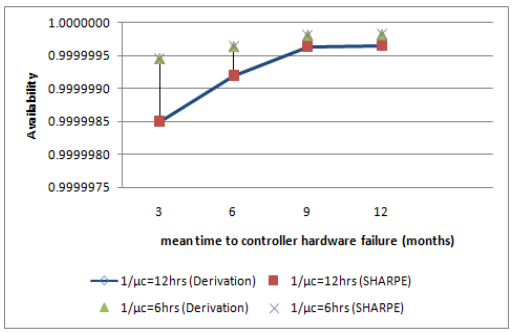

Figure 3. Availability vs different SDN controller hardware repair and failure time

Therefore, the availability is dependent on the SDN controller hardware repair time. The availability is up to 'six nines' which is the best and most expensive of all SLAs for service and application uptime would be an uptime 99.9999% of the time.

The Figure 4 shows the differences in downtime with different SDN controller hardware repair time with different controller hardware failure time. From the result, it is apparent that by using active-active replication of SDN controllers can enhance the availability of IP network.

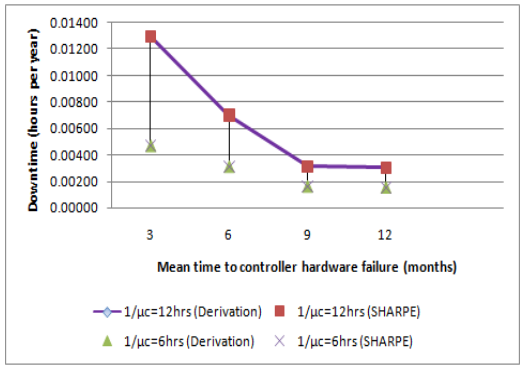

Figure 4. Downtime vs different SDN controller hardware repair and failure time

SHARPE [10] is well known package in the field of reliability and performability. According to Figure 3 and 4, it is found that the derivation results and SHARPE tool simulation results are the same.

5. Conclusion

In this paper, active- active replication of SDN controllers in IP network is presented. This solution is very helpful for enhancing availability for IP network in order to solve hardware and software failure of SDN controller. Proactive software rejuvenation is used for solving software failure. A Markov model of active-active replication for SDN controllers is presented and has shown some numerical results. System availability and downtime for IP network using SDN concept are evaluated. According to the numerical results, combined approach of SDN controller active-active replication and proactive software rejuvenation methodology can enhance the availability of IP network rather than

traditional IP network and can reduce the downtime of the system. Moreover, active-active replication technique for SDN controllers gives guarantee the availability of the services and in order to achieve minimizes the downtime even in case of service restart.

References

[1] Cziva R. , Jou¨et .S. , Stapleton D., Tso F. P., and Pezaros D. P., SDN-based Virtual Machine Management for Cloud Data Centers, Transaction on network and service management.

[2] Eskca E. B., Abuzaghleh O., Joshi P., Bondugula S., Nakayama T., Sultana A., Software Defined Networks' Security: An Analysis of Issues and Solutions, International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015 ISSN 2229-5518

[3] Krpeutz D., Fernando M.V.R, Paulo V., Christian E.R, Siamak A., Steve U., "Software-Defined Networking: A Comprehensive Survey." Proceedings of the IEEE, 2015 103(1): p. 14-76.

[4] Nencioni G., Helvik B. E., Gonzalez A. J., Heegaard P.E. and Kamisinski A., Availability Modelling of Software-Defined Backbone Networks, 46th Annual IEEE/IFIP International Conference on Dependable Systems and Network Workshops, 2016

[5] Nencioni G., Helvik B. E., Gonzalez A. J., Heegaard P.E. and Kamisinski A., Impact on SDN controllers Development on Network Availability, Technical report, 2016

[6] Rout S., Patra S. and Sahoo B., Performance Evaluation of the Controller in Software Defined Networking, 2013 IEEE Symposium on Computers and Communications (ISCC)

[7] Software Rejuvenation. Department of Electrical and Computer Engineering, Duke University, http://www.software-rejuvenation.com/

[8] Sousa P., Bessani A. N., Correia M., Neves N. F., Verissimo P., Highly Available Intrusion-Tolerant Services with Proactive-Reactive Recovery, IEEE Transactions on Parallel and Distributed Systems (Volume: 21, Issue: 4, April 2010)

[9] Thein T. and Park J. S., Availability Analysis of Application Servers Using Software Rejuvenation and Virtualization, J. Computer Science and Technology, 24(2), 2009

[10] Trivedi K. S.. SHARPE 2002: Symbolic Hierarchical Automated Reliability and Performance Evaluator. In Proc. Int. Conference on Dependable Systems and Networks, 2002, pp. 544.

[11] Wang T., Liu F., Guo J. and Xu H., Dynamic SDN Controller Assignment in Data Center Networks: Stable Matching with Transfer, IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications