Proceedings of the International MultiConference of Engineers and Computer Scientists 2016 Vol II,
IMECS 2016, March 16 - 18, 2016, Hong Kong

Software-Defined Assisted PON Multi-DDF Protection and Recovery

Andrew Fernando Pakpahan and I-Shyan Hwang

***Abstract*—EPON system has been chosen as one of the worldwide access network architectures that provide heterogeneous services for multitude users. Fault protection and recovery are some of the mandatory features required to provide certain level of service to its subscribers. The limitation of standardized PON technologies in providing better resiliency in the network brought the need of further enhancement in the PON architecture. Software-defined networking (SDN) brings hope in providing better solutions in managing growing PON architecture, and able to convey new flexible services faster. In this paper an architecture which adds SDN functionalities to a PON is proposed. Simulation results show that our proposed architecture is capable in maintaining overall QoS performance in terms of packet delay, mean jitter, packet loss and throughput.**

***Index Terms*— Network protection, Network recovery, EPON, QoS, Software-Defined Networking, SDN**

I. Introduction

IN the last decade network operators have seen passive optical network (PON) as a solution in providing various kind of services in access network. PON promises larger network capacity in access network infrastructure. Primitively a PON consist of an OLT and multiple ONUs. The OLT is deployed in a centralized location connected to the transport network. Accordingly the optical distribution network (ODN) connects OLT to the ONUs which are installed at various locations nearest to the users. Albeit the 40Gbps capacity of the second next generation PON technology [1], unceasing bandwidth demand from the users has been capacitating network operator to increase its capability to provide more sustaining service. PON users span from home users, small businesses, campuses, enterprises, big data centers, mobile operators, healthcare providers which incorporate enormous end user subscribers. Consequently, a reliable and dependable PON is needed to ensure the service level agreement (SLA) can be satisfied. Types A, B and C of PON protection are defined in ITU-T G.984.1 [2]. Type A protects against failures in the ODN by duplicating all elements in the ODN. Type B protects the OLT and ODN by providing a redundant OLT and ODN configurations with the passive splitter has two input/output ports for the OLT. Type C enhances the protection by adding redundant component in the ONU. In [3], the authors demonstrated Type B protection scheme for time and wavelength division multiplexed PON (TWDM-PON) system to reduce the service outage using ONU holdover procedure. In [4], an in-service integrated fault management mechanism at the distribution drop fibers (DDFs) in EPON is proposed which includes pre-fault and post-fault mechanisms for detection and recovery. The IEEE 1904.1 for Service Interoperability in EPON (SIEPON) [5] accommodates functional requirements to realize service availability guarantee by providing transceiver monitoring, alarm and warnings and optical link protection. Trunk protection and tree protection scheme are presented as optical link protection schemes in SIEPON. The trunk protection scheme is designed to protect the trunk line and the OLT while the tree protection, designed to protect the entire ODN (the trunk and branch segments) along with providing supplementary backup OLT and ONU. Comprehensive protection coverage provided by the SIEPON protection proved very costly due the need to duplicate the entire components involved in the PON. More effective protection solution is provided in [6], instead of using two identical components, ONUs are protected by using protection groups. Two ONUs are coupled and connected via a protection line, thus they are able to protect each other by transmitting its subscriber's packets to the counterpart for failure protection. In fault condition the fault ONU will use the protection line to transmit its traffic and the critical alarm message to the OLT through its couple.

Andrew Fernando Pakpahan and I-Shyan Hwang (ishwang@saturn.yzu.edu.tw) are with the Department of Computer Science and Engineering, Yuan-Ze University, Chung-Li, 32003, Taiwan.

Software-defined networking (SDN) has been an emerging research and industrial interest in the recent years. SDN promises operators better manageability, flexibility, and lower operational expenditure (OPEX) [7]. In SDN perspective the control and data plane functions of each network devices is decoupled. Control plane in a network device need to be programmable and separated from forwarding functions of the data planet. Furthermore, SDN perspective brings a programmable paradigm to the network. SDN's programmable network allows data flows and devices' behavior to be centrally controlled by a single or multiple controllers. SDN capability to modify the control plane in network devices brings the enhancements that are not provided by the current SIEPON or ITU-T standards. In case of fault protection the SDN provides the capability of using its programmable nature to adapt different kind of protection and recovery mechanism. In spite of being applied on big data centers, SDN is being investigated on transport and access network [8]. Using OpenFlow, a prominent programmable network protocol, the authors in [9] improved the use of preplanned backup path using different priorities to guarantee network performance in

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

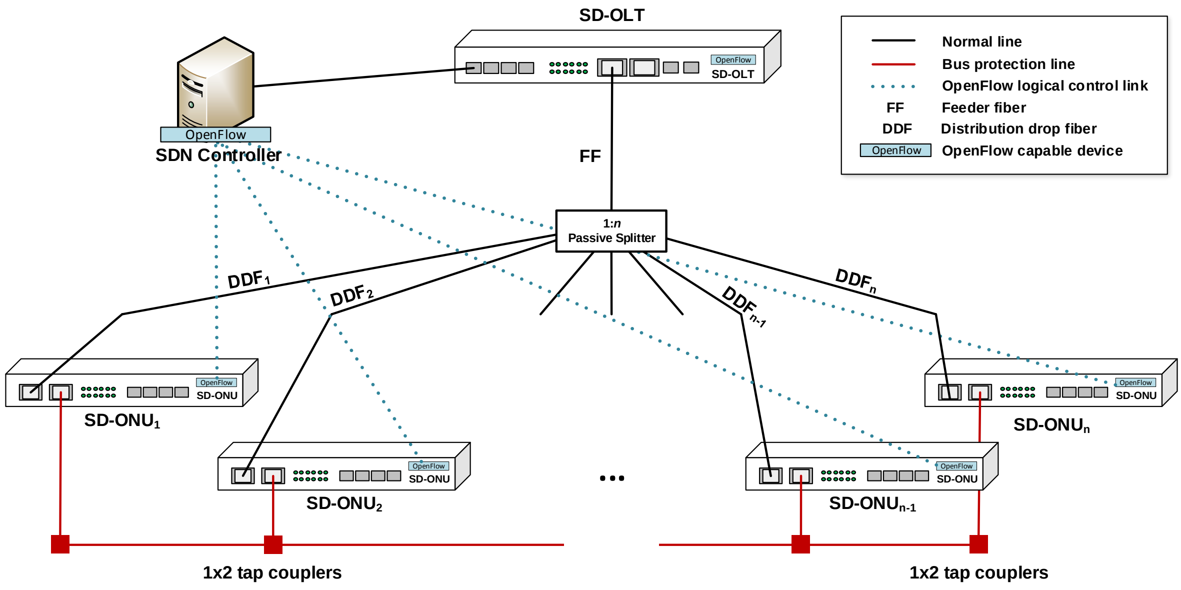


Fig. 1. Proposed software-defined assisted PON multi-DDF protection architecture

achieving fast resiliency. This paper proposes a software-defined assisted PON multi DDF protection where the PON is enriched by the addition of software-defined capability to increase flexibility and manageability in multi-DDF fault condition. The rest of this paper is organized as follows. Section II presents the proposed software defined based assisted PON multi-DDF architecture and mechanism for link resilience and service protection. Section III describes the system performance evaluation and analysis of the proposed mechanism. We conclude the study in section IV.

II. System Architecture and Operations

Fig. 1 presents the proposed software-defined PON multi DDF protection architecture in which OpenFlow functionality is added to every OLT and ONU. The enhanced devices are equipped with the OpenFlow's flow tables and shown as software-defined OLT (SD-OLT) and software-defined ONU (SD-ONU). Furthermore we propose the addition of a bus topology protection line as a backup protection line. The bus protection line connects all ONUs in a single PON using 1 x 2 tap couplers. Bus protection line is used to protect ONU from fault in its normal DDF line or its primary transceiver. The addition of a backup transceiver in every SD-ONU is needed, in which the backup transceiver (L_2-ONU) is connected to the bus protection line and the primary transceiver (L_1-ONU) is connected to the normal DDF line. The SDN controller is vital to facilitate the functionality that is not available in the standardized PON architectures (such as SIEPON) which is the ability to choose the backup ONU in fault condition. The detailed software-defined protection recovery operations are described in the following subsections.

A. *Software Defined Assisted Recovery Mechanism*

SD-ONU and SD-OLT are designed with the aptitude of using SIEPON detection conditions and alarm messages based on the IEEE 1904.1 standard for line fault detection, and the detection parameter is based on "Loss of Signal (LoS)". Before a fault happens the controller has to prepare the protection and recovery mechanism in every devices. The controller has the knowledge of the network topology by acquiring the flow table entries from every devices using the OPFT_GET_CONFIG message. The flow statistics afterward are gathered using the OFPT_STATS message. This additional information is used to decide the best protection and recovery mechanism that can be implemented. Furthermore the controller can prepopulate the flow tables with the necessary protection scenario. The controller provides each ONU with different paths to transmit its subscribers' packets by inserting flow entries in the ONU flow table using the OPFT_FLOW_MOD message. The detailed operation of the recovery preparation in controller can be seen in Fig. 2. Every SD-ONU can be assigned as backup ONU and capable of providing backup protection in case of fault happens in other ONU(s). Based on the flow table, a faulty ONU can use the backup protection line to transmit its traffic to the backup ONU in

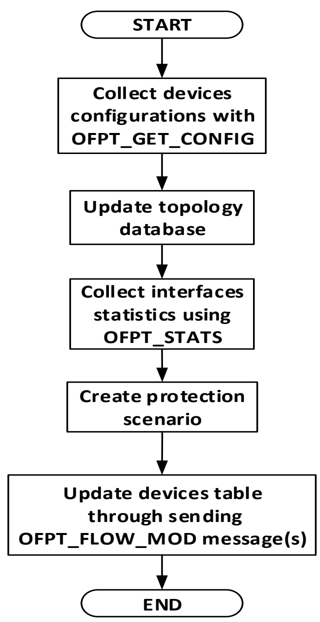


Fig. 2. Detailed operation of the controller in fault protection preparation

fault condition. For easy understanding of the flow table working mechanism, Table I provides a simplified flow table for an ONU in case of DDF fault. In upstream direction the ONU has two paths available with different priority. Different priority in the flow table ensures different paths can be taken if a failure is detected in its normal line. In case of an ONU detects fault in its normal transmission line (L_1-ONU), based on the flow table, the ONU automatically switches its subscribers traffic to the backup protection line using its L_2-ONU and sends a new OPFT_PORT_STATUS message to the controller through the assigned backup ONU. The backup ONU then forwards the faulty traffic (traffic from ONU(s) in fault condition) to the OLT and the fault message afterward is received by the controller. Knowing an ONU in faulty condition and is currently using the backup ONU for transmitting the OLT, the controller instructs the OLT to adjust the dynamic bandwidth allocation (DBA) to provide more transmission window to the backup ONU. The detailed controller actions in fault condition is shown in Fig. 3.

TABLE I.
FAULT ONU FLOW TABLE IN DDF FAULT CONDITION

Out Interface	Desti-nation	Priority	Port Status	Selected
L_1-ONU	Primary OLT	High	Failed	
L_2-ONU	Backup ONU	Normal	Active	Y

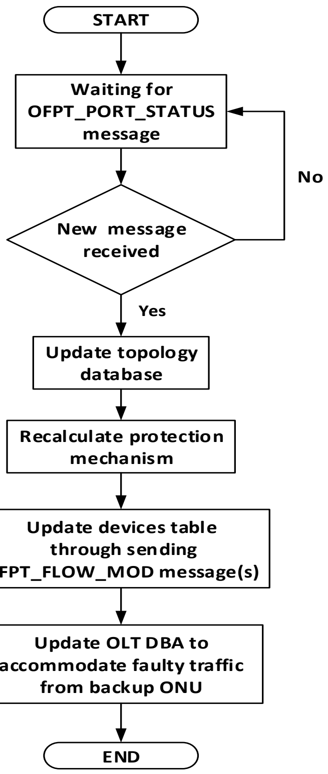


Fig. 3. Detailed operation of the controller in fault condition

B. *Software-Defined Fault DBA (SD-FDBA)*

For providing better service in fault condition, in the proposed architecture, upon receiving instructions from the controller, the OLT adjusts the transmission window allocation for the backup ONU. OLT assigns more bandwidth to the backup ONU according to the number of faulty ONU(s) it handles. The proposed software-defined fault DBA (SD-FDBA) is an offline DBA, the DBA grants a bandwidth based on the bandwidth available, $B_{available}$ and the maximum transmission window, W_{max}. W_{max} for each traffic type is assigned depending on the traffic priority (EF, AF, BE). The DBA needs to satisfy highest priority (EF) traffic first, then assigns the remaining bandwidth allocation to the mid (AF) and low (BE) priority. The EF is always served first because in case of service disruption many of the transmission involved the emergency contact 911 services [10]. In DDF fault condition SD-FDBA is applied by increasing the available guaranteed bandwidth B^{min}, according to the number of ONU in a PON and also the number of DDF fault, which is expressed as Eq. (1),

$$B^{min} = B_{available} * \frac{N+1}{n}, \quad (1)$$

where N is the number of DDF fault in a single PON and n is the number of ONU in a single PON.

III. PERFORMANCE EVALUATION

In this section, the proposed architecture is evaluated in terms of mean packet delay, jitter, packet loss and system throughput performance. The proposed system model is demonstrated using an OPNET simulator with an OLT with 8 ONUs. The downstream and upstream transmission capacity between the OLT and ONU is set to 1 Gbps. ONUs distance with the OLT is uniform over the range from 10 to 20kms, and each ONU has 10Mb buffer size [11,12]. Moreover, the self-similarity and long range dependence are used to model the network traffic of the AF and BE, respectively [13]. This model generates highly bursty AF and BE traffics with a Hurst parameter of 0.7. The packet size is uniformly distributed between 64 and 1518 bytes. The high-priority traffic, i.e, EF traffic, is modeled using a T1 circuit-emulated line with IP/UDP encapsulation and a constant frame rate (1 frame/125µs) with a fixed packet size (70bytes). The simulation scenario is summarized in Table II. Two different scenarios are designed and analyzed for various EF service, AF service, and BE service proportions as shown in Table III

TABLE II.
SIMULATION PARAMETERS

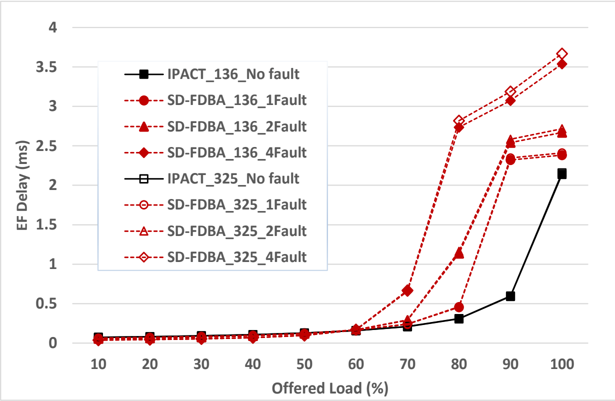
Parameters	Value
Number of ONUs	8
Up/Down link capacity	1Gbps
OLT-ONU distance	10-20km
ONU buffer size	10Mb
Maximum transmission cycle time	1.5ms
DBA Guard time	1μs
DBA Computation time	10μs
Control message length	0.512μs
Number of DDF faults	1, 2, 4 Faults

TABLE III.
Simulation Scenario for Different Traffic Proportions

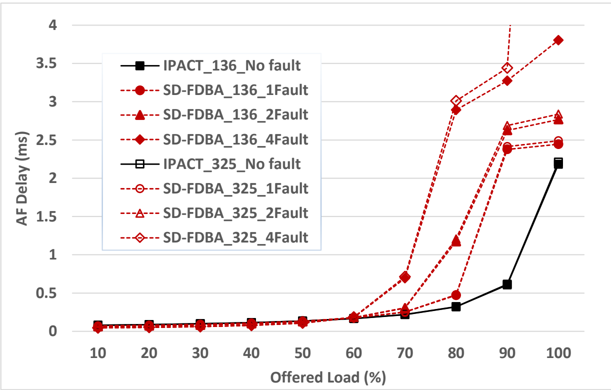
	EF (%)	AF (%)	BE (%)
Scenario1 (136)	10	30	60
Scenario2 (325)	30	20	50

A. *Mean Packet Delay*

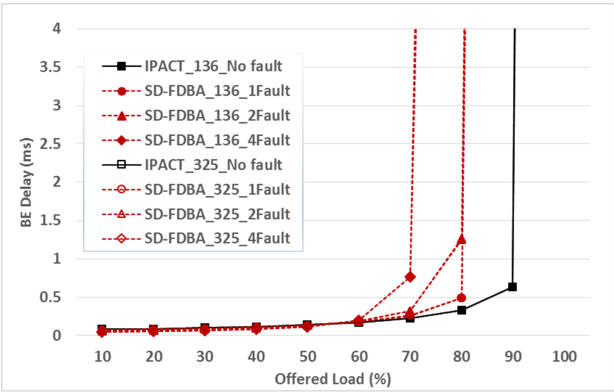
Fig. 4 shows the overall packet delay in different traffic loads for EF, AF and BE. The No_fault scenario with different traffic proportions has the lowest overall packet delay in every scenario. In fault condition, the delay are consistently higher due to the necessity of the backup ONU to handle the additional incoming faulty traffic from the faulty ONU. More fault incurred more delay. However, the proposed SD-FDBA still guarantee to maintain EF delay, which is less than 5ms.



a) Comparison of average EF delay for different traffic proportions



b) Comparison of average AF delay for different traffic proportions



c) Comparison of average BE delay for different traffic proportions

Fig. 4. Average delays of IPACT and SD-FDBA in different traffic loads.

B. *Jitter*

Fig. 5 shows the mean EF jitter versus the offered load in different scenarios. The EF jitter in fault scenarios are consistently higher than the original IPACT. The EF jitter decreases when the EF traffic ratio is increased.

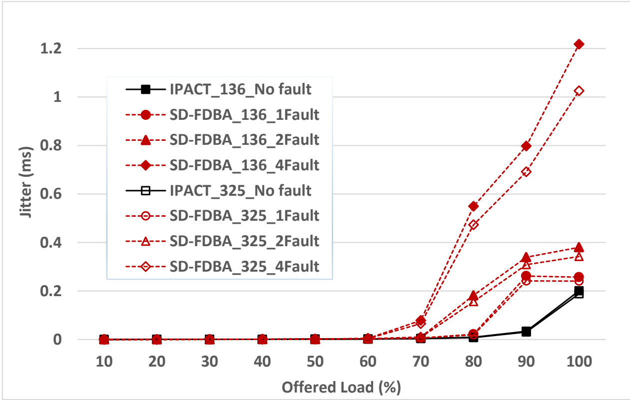


Fig. 5. EF jitter performance comparison of IPACT and SD-FDBA and IPACT in different traffic loads.

C. *Packet Loss*

Fig. 6, depicts the overall packet loss probability in different scenarios. There is no packet loss when the traffic load is less than 60%; however, in 4 fault condition the packet drop begins the happen when the load is more than 70% because the ONU buffer is not capable of handling the additional traffic from the faulty ONU.

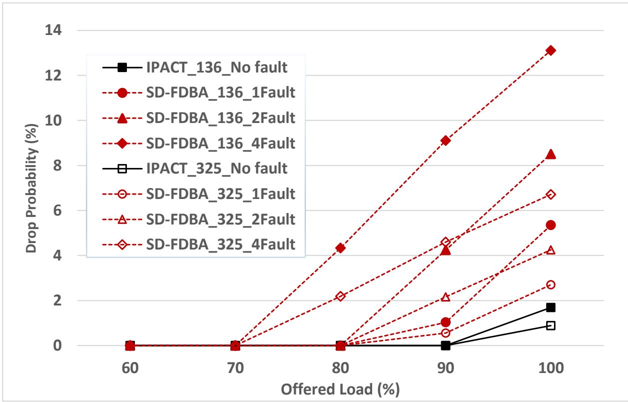


Fig. 6. Drop probability in different traffic scenarios.

D. *System Throughput*

As depicted in Fig. 7, the more faults occurred in a PON, the higher the throughput. The reason the throughput is higher in fault condition lies in the scheduling overheads and the number of ONUs. When failures occur in the network, less the number of ONU is connected to the OLT, thus the upstream scheduling overheads are decreased and the net throughput are increased.

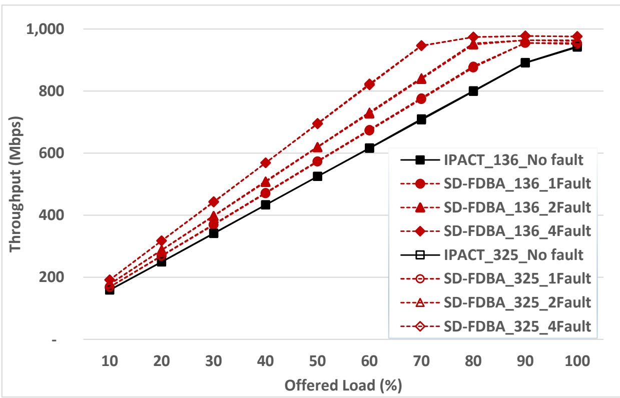


Fig. 7. Net throughput in different scenarios.

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

IV. Conclusion

This paper has proposed a software-defined assisted multi DDF protection against optical distribution network (ODN) failures, such as the drop distribution fiber (DDF) failures and ONU(s) transceiver failures. The proposed mechanism uses resilience and service protection as defined in IEEE 1904.1 SIEPON with the addition of SDN capabilities to remotely modify the flow table in the OLT and ONU. DDF failure(s) is handled by a backup ONU as a temporary intermediator to link its subscriber to the OLT. Simulation results have shown that the proposed architecture and mechanism can still guarantee the overall QoS.

References

[1] D. Nesset, "NG-PON2 Technology and Standards," *IEEE/OSA Journal of Lightwave Technology*., vol. 33, no. 5, pp. 1136–1143, Mar. 2015.

[2] "Gigabit-capable passive optical network (GPON)," ITU-T recommendation G.984, 2008.

[3] T. Nishitani, J. Mizuguchi, and H. Mukai, "Experimental study of type B protection for a TWDM-PON system [Invited]," *IEEE/OSA Journal of Optical Communications and Networking,* vol. 7, issue 3, pp. A414-A420, Mar. 2015.

[4] A.T. Liem, I.S. Hwang, A. Nikoukar, and M.S. Ab-Rahman, "Distribution drop fiber in-service fault management in enhanced EPON system," *Optical Switching and Networking*, vol. 17, pp. 52-63, July 2015.

[5] IEEE P1904.1 Standard for Service Interoperability in Ethernet Passive Optical Networks, July 2013.

[6] A.T. Liem, I.S. Hwang and A. Nikoukar, "An autonomous recovery mechanism against optical distribution network failures in EPON", *Optical Fiber Technology*, vol. 20, issue 5, pp. 552-560, Oct. 2014.

[7] E. Hernandez-Valencia, S. Izzo, and B. Polonsky, "How will NFV/SDN transform service provider opex?," Netw. IEEE, vol. 29, no. 3, pp. 60–67, 2015.

[8] D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[9] A. Sgambelluri, A. Giorgetti, F. Cugini, F. Paolucci, and P. Castoldi, "OpenFlow-based segment protection in Ethernet networks," *IEEEOSA J. Opt. Commun. Netw.*, vol. 5, no. 9, pp. 1066–1075, Sep. 2013.

[10] M.A. Esmail, H. Fathallah, Physical layer monitoring techniques for TDM-passive optical networks: a survey, IEEE Commun. Surv. Tutorials 15 (2) (Jan. 2013) 943–958.

[11] I.S. Hwang, A. Nikoukar, C.H. Teng, K.R. Lai, Scalable architecture for VOD service enhancement based on a cache scheme in an ethernet passive optical network, IEEE/OSA J. Opt. Commun. Networking 5 (4) (April 2013) 271–282.

[12] G. Kramer, B. Mukherjee, S. Dixit, Y. Ye, R. Hirth, Supporting differentiated classes of service in ethernet passive optical networks, J. Opt. Networking 1 (8) (Aug. 2002) 280–298.

[13] G. Kramer, Ethernet Passive Optical Network, McGraw-Hill Professional, 2005.