NVEO
Natural Volatiles & Essential Oils

Security Enhanced Forward Compatible Integrated Asynchronous GPON and XGPON using Pseudo User Scheme

Karanvir Mangal
Department of Electronics and Communication Engineering
Thapar Institute of Engineering & Technology
Patiala (147004), Punjab, India
karanvirmangal@gmail.com
Hardeep Singh
Department of Electronics and Communication Engineering
Thapar Institute of Engineering & Technology
Patiala (147004), Punjab, India
hardeep@thapar.edu

Abstract—
Security of the proposed Passive Optical Network is increased manifolds without any interference with the transmission line by co-transmitting Pseudo User Cross-Correlation based Diagonal Double Weight Codes, making detection obscure at eavesdropper receiver.

Keywords—Passive optical networks (PON), Diagonal double weight (DDW), Pseudo user scheme (PUS), Continuous wave (CW), X Gigabit passive optical networks (XGPON), Optical network unit (ONU), Single mode fiber (SMF), Spectral amplitude coding optical code division multiple access (SAC-OCDMA), Optical line terminal (OLT), Bit error rate (BER), Downstream (DS), Upstream (US)

I. INTRODUCTION

Until today, most of the work has been reported for the improvement of capacity and transmission rate in PONs, although data confidentially of available data is major work which needs to be addressed either. Eavesdropping seriously influences the performance of the system and exposes the confidential information of authorized user. In this paper, a novel security enhanced pseudo user scheme against eavesdropping in forward compatible asymmetrical GPON/XGPON is presented which is less complicated than techniques used in [1-2].

II. PSEUDO USER SCHEME PRINCIPLE IN FORWARD COMPATIBLE GPON/XGPON

In order to provide extra security to a system, pseudo random users are transmitted along with GPON and XGPON, hence it becomes extremely difficult for eavesdropper to get correct information. Therefore, DDW codes are incorporated in the system. Probability of GPON (P(GPON)) for '0' and '1' is 1/2 and if PUS at same data rate is employed in the system, then total cases become P(Total)=P(GPON) x P(PUS)=1/4 while the data rate of XGPON is 4 times the data rate of GPON, so total number of cases at which 1s and 0s occur at same time is 1/16 (0000 to 1111). Thus, for XGPON with PUS, the total cases

become P(XGPON) x P(PUS)=1/16 x 1/16 (1/16 because PUS and XGPON are operated at 10 Gbps) =1/256. Hence total number of cases including GPON, XGPON and PUSs becomes 1/1024. Hence, it is very hard for the eavesdropper to grasp correct information.

III. SIMULATION SETUP

A security enhanced forward compatible GPON/XGPON system is demonstrated under the existence of eavesdropper as depicted in Fig. 1. A CW laser at wavelength of 1490 nm is incorporated in the system for GPON transmitter. Similarly, a laser at wavelength of 1577 nm is employed for XGPON transmitter. Bit streams are generated from pseudo random bit sequence generator and multiplexed signals are fed to bi-directional fiber (SMF-28). After transmission over SMF, signals are passed through two optical filters so that GPON and XGPON wavelengths get separated. Both the wavelengths are made to fall on photo-detectors and noise suppression is done with low pass filters. Decision of quality received and errors are observed from BER analyzer. Wavelengths 1270 nm (XGPON) and 1310 nm (GPON) are used for upstream. At downstream, two pumps at 1240 nm and 1206 nm are used to give Raman gain to upstream wavelengths. An upstream decoder with photo-detector, low pass filter and 3R generator is employed at receiver end.

For the integration of PUS scheme with aforementioned system, a spectral amplitude coded OCDMA system is incorporated. One SAC-OCDMA user is assigned for GPON and another for XGPON to boost the security of the system both in OLT and ONU. A system is proposed with DDW codes [3] having cross-correlation 1.

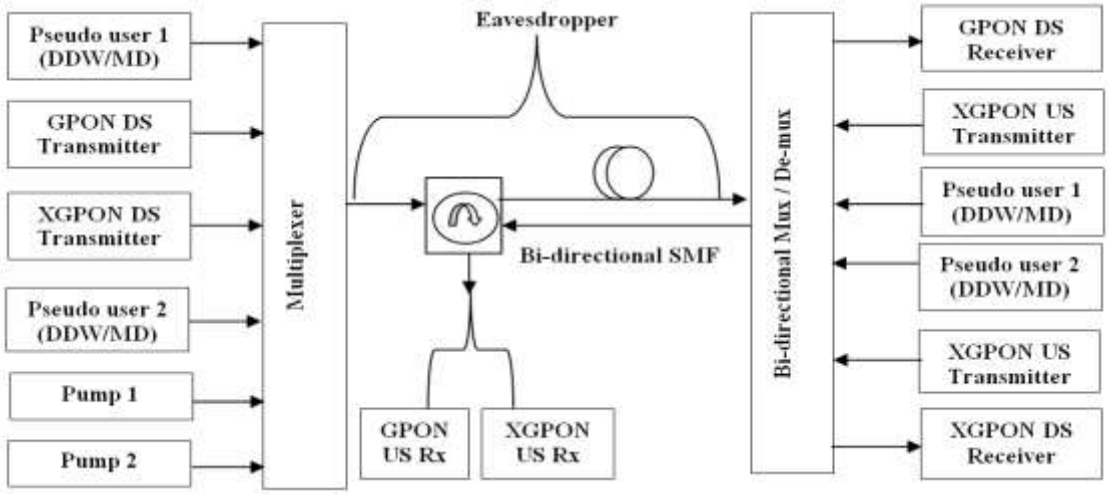

Fig. 1. Block diagram of security enhanced forward compatible co-existed GPON/XGPON system

IV. RESULTS AND DISCUSSIONS

Investigation of the proposed system has been done using simulation software Optiwaves's Optisystem™. Table I. shows values of the Q factor and Table II. shows BER with the variation of the launched power at the eavesdropper. Readings are observed in with and without pseudo random user scheme at eavesdropper's receiver.

Obviously, more Q factor and less BER are observed at the eavesdropper in the system where PUS is not used. This is due to less scrambling of data because no false user is there to minimize the probability of detection for the unauthentic user. However, less Q factor and more BER are seen at the eavesdropper when PUS is included.

TABLE I. VALUES OF Q FACTOR VERSUS LAUNCHED POWER AT EAVESDROPPER

Launched Power (dBm)	**Q Factor (Eavesdropper in without PUS system)**	**Q Factor (Eavesdropper in with PUS system)**
-2	5.55	3.16
0	6.03	3.60
2	6.64	4.03
4	7.41	4.37
6	8.38	4.57

Significantly, with increase in the input power of authentic users, probability of code word detection at eavesdropper's decoder increases. Presence of pseudo user does not compromise with quality of signal received by the authentic user. Therefore, for enhanced security, PUS should be included in the system.

TABLE II. VALUES OF BER VERSUS LAUNCHED POWER AT EAVESDROPPER

Launched Power (dBm)	**BER (Eavesdropper in without PUS system)**	**BER (Eavesdropper in with PUS system)**
-2	10^{-8}	10^{-4}
0	10^{-10}	10^{-4}
2	10^{-11}	10^{-5}
4	10^{-14}	10^{-6}
6	10^{-17}	10^{-6}

V. CONCLUSIONS

In this paper, an integrated novel security enhanced forward compatible GPON/XGPON is presented with pseudo random scheme to resolve the network breaking issue because of eavesdropping. The presence of pseudo user with false wavelength makes deciphering the information bits tedious for eavesdropper. Thus, proposed system is flexible, security enhanced and reliable for PON systems.

REFERENCES

[1] Yaoqiang, Xiao. *et al*., "Two-level encryption for physical-layer security in OFDM-PON based on multi-scrolls system", optics communications, vol. 440, pp. 126-131, June 2019.
[2] K, Gao. *et al*., "Optical code division multiple access secure communication systems with rapid reconfigurable polarization shift key user code", Opt. Eng., vol. 54, no. 9, 096101, Sept. 2015.
[3] Gurpreet Kaur, Gurinder Singh, "Performance analysis of SAC-OCDMA in free space optical medium using MD and DDW code," in Recent Advances in Engineering and Computational Sciences, (IEEE, Chandigarh, India 2015).