Chapter 4
Applying Smart Security Model to Protect Client Services From the Threats of the Optical Network

Kamel H. Rahouma
Minia University, Egypt

Ayman A. Ali
Minia Unversity, Egypt

ABSTRACT

The chapter discusses the security of the client signals over the optical network from any wiretapping or loosing. The physical layer of the optical transport network (OTN) is the weakest layer in the network; anyone can access the optical cables from any location and states his attack. A security layer is proposed to be added in the mapping of OTN frames. The detection of any intrusion is done by monitoring the variations in the optical signal to noise ratio (OSNR) by using intelligent software defined network. The signal cryptographic is done at the source and the destination only. The chapter shows how the multi-failure restorations in the multi-domains could be done. A new model is introduced by slicing the multi-domains to three layers to fit the needs of 5G. The results show that the multi-failure restoration improved from 25% to 100%, the revenue from some OTN domains increased by 50%, the switching time enhanced by 50%, the latency reduced from 27 msec to 742 usec, and it will take many years to figure out the right keys to perform the decryption process.

DOI: 10.4018/978-1-7998-2795-5.ch004

INTRODUCTION

Applying 5G and beyond technologies require to exchange an enormous amount of data between various locations inside any country and globally. Transporting all of these amounts of data in the access networks is easier than to transport it across a backbone network (Palattella et al., 2016). There are many advanced technologies which are used to transfer the data over the backbone network, which begin from the Plesiochronous Digital Hierarchy (PDH), the Synchronous Digital Hierarchy (SDH) and finally the most advanced technology of the data transmission is the Optical Transport Network (OTN) over the Dense Wave Division Multiplexing (DWDM). The high capacities of the OTN circuits can provide the suitable infrastructure to lead the breakthrough in the access and the mobile networks such as 5G and beyond 5G technologies, which need to transfer a massive amount of data of many smart applications between the different sites even though these sites are separated by very long-distances or separated by the borders between the different countries around the world (Monteiro, Gameiro, & Hu, 2016).

As the OTN is extending over thousands of kilometers of distances, which covers most of the area of any country, it carries all the services of the telecom operators from the different mobile applications, the enterprise services, and the Internet services. Although the OTN plays an essential role in carrying most of all the traffic of the different communication technologies in the country, many threats can affect this great job of the OTN; one of these threats is the customer's data, which are carried over the OTN, may be lost due to one or more fault in the working and protection routes of the optical network, another threat which can affect the customer's data over the OTN is the physical layer of the OTN is natural to be intruded from any place in the network routes by a 3rd party who is not authorized (Wetterwald, Saucez, Nguyen, & Turletti, 2016).

Many kinds of research discussed the threads of the optical network separately, one of these studies proposed the implementation of the OTN encryptions as point to point provisioning and wavelength level encryptions which are fitted demands in the complete line rate with the sub wavelengths demand, the encryptions of the aggregations and grooming are preferred to increase the utilization of the network and to decrease the complexity of the management system (Guan, Kakande, & Cho, 2016). Another study investigated that the authorized user wants to choose the proper channel coding to manage the secrecy capacity, while other security evaluation parameters are necessary to be applied to estimate the data security and the stability of the system. The protection leakage determinant is employed to assess the physical-layer safety level while the secure receiving range is employed to estimate the protection transmission scope, and the impacts of the extraction position, the extraction degree, the number of the users, and the length of the encryption key