How to Increase Key Space in PON

Asad Ali, Ghulam Ali, Noor Ahmed Shaikh
School of Electrical Engineering and Computer Science
National University of Science and Technology, (NUST)
Islamabad, Pakistan.
Email: asad.ali@seecs.edu.pk

Abstract: key space has always remained a concern in all the cryptographic systems. In today's fast computing world, key space is always limited. Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES) have solved the problem to a greater extent. However, In this paper, we introduce a novel mechanism which increases the key space in Passive Optical Network (PON) by using wavelength hopping using wavelength Division Multiplexed system in the PON instead of Time Division Multiplexed system. Mathematical results show that we achieve many times more key space then DES, Triple DES, AES.

Keywords: Key Space, DES, Triple DES, AES, PON.

I. Introduction

There has always been increased in the demand of bandwidth of the communication line. The demand for faster and more efficient communications systems is always growing. Traditional "Quad-play" applications [1] (which refer to a bundle of services with voice, video, Internet, and wireless) and premium rich-media applications (e.g., multimedia, interactive gaming, and metaverse) need to be delivered to the end users in a satisfactory and economical way. So the need to design an efficient first mile network is accelerating by leaps and bound. Thus all these give rise to a new Optical Passive Optical Network (PON). PON [10] consists of a central office (CO) in which there resides an Optical Line Terminal (OLT). This OLT is connected to different Optical Network Units (ONU) through a trunk fiber. There is an optical splitter between the OLT and the ONUs. The distance between the OLT and the ONUs is typically 20kms. A single OLT can support up to 32 ONUs over the distance of 10kms. The number of ONUs supported decreases as the distance between the OLT and the ONUs is increased. Since PON is all-passive, so therefore it is more robust as well.

For data communication [10, 11] in upward direction, the message is simply unicast to OLT though the trunk fiber. However, in downward direction a single message is sent to all ONUs through trunk fiber regardless of the targeted ONU. The optical splitter splits the message signal equally among all ONUs. All the ONUs get the message, all the ONUs discard the message except the one for the message is intended. Since downstream traffic is broadcast, all the ONUs get the message from OLT, so eavesdropping can happen when an unintended ONU receive the message packet and spoil its contents. So this is clearly a major security issue. It's quite easy for malicious user to reprogram ONU to capture desired frames. Steps must be taken so that an unintended ONU could not open the packet and only the desired ONU for which the packet is meant may open the packet. SO in this regard, downstream data packets must be encrypted using certain keys. Only the intended recipient ONU should have information about the secure key. So that unintended ONUs may not be able to send decrypt the data. So in this regard, the key space always plays a key role in the security of communication. The number of keys, that is, the key space used to encrypt the confidential data is always limited. Particularly with the advent of fast computational devices it is very easy to come up with the key being used for transmission by both the parties. Therefore a large key space is always desired in this regard. So that third party may not come to know about the key. Larger the key space, the secure will be the communication.

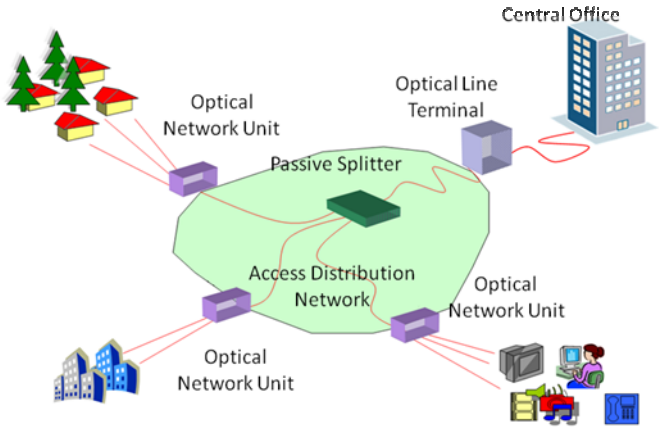

Figure 1: A Typical PON

Rest of the paper is organized as follows. Section II highlights the current security measures that have been taken to cater the security issues in PON, in section III we show our proposed mechanisms, and then finally conclusion in section V.

II. Current Security Measures in PON

There are so many flavors of PON like Ethernet PON (EPON), Broadband PON (BPON), Gigabit PON (GPON), but there is no standard defined by IEEE for secure end to end communication except for GPON. Therefore vendors use their own algorithms for providing secure end to end communication. The IEEE 802.3ah EPON standards do not specify any authentication and encryption mechanisms [7, 8]. Thus, particular proprietary solutions have been implemented by EPON manufacturers [9]. Encryption method can also be supplement with IPsec or MACsec. The ITU G.983 BPON recommendations do not specify particular security mechanisms either [7, 8], but its successor; the ITU G.984 GPON recommendations do use the Advanced Encryption Standard (AES) for downstream transmission. Although AES does solve the key space problem up to greater extent, but in our proposed scheme, we produce many time larger numbers of keys then AES.

III. Proposed Mechanism

International Telecommunication Union-Telecommunication Standardization sector (ITU-T) defines various usable frequencies [5], channel frequency spacing and center frequency. In a WDM system, the number of channels available depends upon the spacing among the channels. Greater the spacing among the channels smaller will be the number of channel available. For example the ITU draft standard G.692 defines WDM system with channel spacing of 100GHz with a center wavelength of 1553.52 [7,8]. For channel spacing of 100GHz the available usable channels are 45. As shown below in the diagram.

Frequency (THz^1)	Wavelength (nm^2)	Frequency (THz)	Wavelength (nm)	Frequency (THz)	Wavelength (nm)
196.1	1528.77	164.6	1540.56	193.1	1552.52
196.0	1529.55	194.5	1541.35	193.0	1553.33
195.9	1530.33	194.4	1542.14	192.9	1554.13
195.8	1531.12	194.3	1542.94	195.8	1554.94
195.7	1531.9	194.2	1543.73	192.7	1555.75
195.6	1532.68	194.1	1544.53	192.6	1556.56
195.5	1533.47	194.0	1545.32	195.5	1557.36
195.4	1534.25	193.9	1546.12	192.4	1558.17
195.3	1535.04	193.8	1546.92	192.3	1558.98
195.2	1535.82	193.7	1547.72	192.2	1559.79
195.1	1536.61	193.6	1548.51	192.1	1560.61
195.0	1537.40	193.5	1549.32	192.0	1561.42
194.9	1538.19	192.4	1550.12	191.9	1562.23
194.8	1538.98	193.3	1550.92	191.8	1563.05
194.7	1539.77	193.2	1551.72	191.7	1563.86

Figure 2: Various Channels Obtained With Channel Spacing of 100GHz According to G.692 Standard [5].

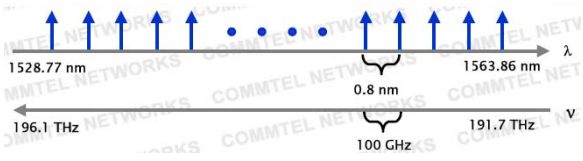

Figure 3: Channel Ranges for Channel Spacing of 100GH

Now if we put the above channels (wavelengths) in the form of a 15x3 matrix, as shown in Figure 3 below, the matrix will show various available channels. The matrixcan be changed by simply permuting the elements of the matrix, that is, by

permuting the wavelengths. If ‘a’ denotes the number of rows and ‘b’ denotes the number of columns of a matrix, then we get $(a!)^b$ unique matrices. For 15x3 matrcxes, we get 2.236×10^{36} unique matrices. So even ifwe use a unique key for every packet, as is the case in churning in BPON, then we would be able to send 2.236×10^{36} different packet. One interesting point here is that if we keep on changing the key on hourly bases, then we’ll have 2.545×10^{32} years before the first key is used for the second time, in other words, before the first key is reused. So it is such a big time—such a big key space. Similarly if we use G.694.1 standard, which provide channel spacing of 25GHz and thus gives 169 channels. If we put these 169 channels into the matrix of 13x13, and want to find the maximum permutation and thus maximum unique matrices, in other words, maximum keys, using $(a!)^b$, we’ll get 2.1166×10^{127} Which is again such a big key space, many times larger then DES or AES.

$$\begin{bmatrix} 1528.77 & 1552.52 & 1540.56 \\ 1529.55 & 1553.53 & 1541.35 \\ 1530.33 & 1554.13 & 1542.14 \\ 1531.12 & 1554.94 & 1542.94 \\ 1531.9 & 1555.75 & 1543.73 \\ 1532.68 & 1556.56 & 1544.53 \\ 1533.47 & 1557.36 & 1545.32 \\ 1534.25 & 1558.17 & 1546.12 \\ 1535.04 & 1558.98 & 1546.92 \\ 1535.82 & 1559.79 & 1547.72 \\ 1536.61 & 1560.61 & 1548.51 \\ 1537.40 & 1561.42 & 1549.32 \\ 1538.19 & 1562.23 & 1550.12 \\ 1538.98 & 1563.05 & 1550.92 \\ 1539.77 & 1563.86 & 1551.72 \end{bmatrix}$$

Figure 4: Matrix of the Channels.

IV. Conclusion

In this paper we have shown a fine technique of increasing the key space for Passive Optical Networks. We showed that if we use WDM instead of TDM in PON and put the available channels in a form of a matrix and use that matrix as a key, and permute the entries of the matrix then the number of keys significantly increases. The number of channels increases as the channel spacing decreases, thus the number of key increases.

V. Acknowledgement

This is the extended version of our own paper presented and published as Conference proceedings in “International Conference on Computers & Emerging Technologies” (ICCET 2011) held on 22-23 April 2011 at Shah Abdul Latif University, Khairpur, Sindh, Pakistan

References

[1] Glen Kramer, Biswanath Mukherje, Gerry Pesavento, “IPACT: A dynamic protocol for an Ethernet PON (EPON)”, IEEE Communications Magazine, 2002

[2] Glen Kramer et. al., “Multipoint Control Protocol (MPCP) Common Framework”, 2001 (Presentation)

[3] Bob Gaglianello, “Multipoint Control Protocol for EPONs”

[4] Dense Wavelength Division Multiplexing by Commtel Networks

[5] Thomas H. Shake,” Security Performance of Optical CDMA Against Eavesdropping“, JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 23, NO. 2, February 2005.

[6] International Telecommunication Union-Telecommunication Standardization sector (ITU-T), G9831 standard, “Broadband optical access systems based on Passive Optical Networks (PON)”, October, 1998.

[7] International Telecommunication Union-Telecommunication Standardization sector (ITU-T), G984.1 standard, “Gigabit-capable Passive Optical Networks (GPON)”, March 2003.

[8] A. Teixeira et all “Security Issues in Optical Networks Physical Layer” ICTON 2008.

[9] IP over WDM, by Sudhir Dixit. Willey Interscience, 2003 John Wiley And Sons.