A CDMA Secure Optical Access Network

Ortega A. Alfredo, Victor A. Bettachini, José Ignacio Alvarez-Hamelin, Diego F. Grosz

A CDMA Secure Optical Access Network

A. A. Ortega[1,2] , V. A. Bettachini[2], J. I. Alvarez-Hamelin[2,3], D. F. Grosz[2,3]

(1) Core Security Technologies, Humboldt 1967 1° p, C1414CTU Buenos Aires, Argentina

(2) ITBA, 25 de Mayo 444, C1002ABJ Buenos Aires, Argentina

(3) CONICET (Argentinian Council of Scientific and Technological Research)

aortega@alu.itba.edu.ar, {vbettachini,ihameli,dgrosz}@itba.edu.ar

Abstract

We propose a OCDMA network implementation that enhances security, using a star topology of up to 128 ONUs covering 20 km, with applications to metro-Ethernet. Numerical simulations demonstrate the feasibility of the proposed scheme.

Keywords: Optical security and encryption; Networks, combinatorial network design

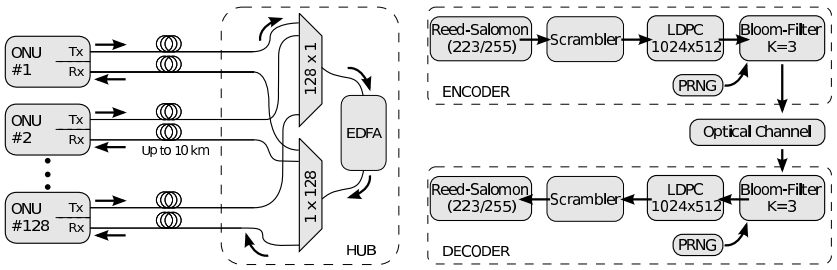
1 Introduction

Modern passive optical networks provide a method for fast and reliable voice and data communication between multiple premises. However, communication methods employed today are inherently insecure, as they don't provide privacy from a sufficiently motivated eavesdropper, as signals are broadcasted to all ONUs. Communication security must be implemented by the end-points on higher-level protocols, and are often neglected. This paper aims to improve the immunity of optical networks to a variety of attacks. Inspired on a Passive Optical Network, we present a solution for this problem using CDMA for the data codification, specifically a time-hopping algorithm at the bit-level. In contrast to other metro optical network designs [3], we propose a star network topology, using a single-laser wavelength and providing security at physical level. This allows low-cost private networks or point-to-point channels to be set up between ONUs up to 10 km from the optical Hub.

In classic TDMA, a medium is shared between several channels. The slots are assigned in a way totally predictable for all ONUs in the network. Thus an optimal medium utilization is achieved, but security and privacy are compromised because no safeguard are made against a malicious ONU accessing the network. Any endpoint has complete access to all channels in this broadcast medium. We present a simple method to assign pseudo-randomized slots to every channel, so that only authorized ONUs can decode the channel: Each channel is assigned a Pseudo-random generator algorithm (not necessarily the same). Two or more channels must share the secret key (usually the seed) of the PRNG to make the slot sequence predictable and communication between them possible. The PRNG algorithm must be cryptographically secure. Several known algorithms exists that meet these criteria [5]. In our simulation, we consider the optical fiber as a Z-channel [4] (only a bit 0 can be overwritten for a bit 1), and we apply error-correction codes required for reliable communications in the presence of collisions, which happen in pseudo-randomly chosen time slots. Finally, as this protocol works at the lowest level of the OSI model, link-layer, any higher level protocols like Ethernet or ATM can be implemented on top with no modifications, but the enhanced confidentiality supports additional protocols like secure VLANs, not possible with common PON architectures.

2 Architecture

The proposed system is composed of an access layer, where CDMA and error correction are implemented, and a physical layer based on an optical network with certain similarities to PONs.



(a) Optical Layer (b) Access Layer

Fig. 1. Proposed network design

The access layer is implemented using time-hopping CDMA, where each of the 128 possible on-line ONUs sends bits in a slot chosen randomly from a frame of 330 slots, therefore collisions between different ONUs will happen and error correction must be used to guarantee error-free data transmission. Notice that the synchronization is done at slot level only because transmissions of each ONU are random, in contrast to TDMA where the synchronization is also done at frame level. Moreover, each ONU can send data at any time, in contrast to TDMA where ONUs send data continuously; this feature is very useful to transport Ethernet frames. A certain ONU X can receive messages from an ONU Y if X has the *key* of Y, and vice versa. Therefore, if a certain group of ONUs were to communicate over a VLAN, it is needed that everyone in the group knows the other's *keys*. ONUs' data streams are treated with the following error correction techniques: Reed-Solomon (223/255) and LDPC (matrix of 1024×512) algorithms (see [6] and references therein), and bloom-filters [2], with $K = 4$. The choice of these correction algorithms was heavy influenced by modeling the optical fiber as a Z-channel, having a Shannon limit of $C_Z = \log_2\left(1 + (1-p)p^{p/(1-p)}\right)$, where p is the probability of error. This capacity limit is larger than that of a symmetric memory-less binary channel [8].

Optical transmission is performed by a 2 dBm 1550 nm DFB-LD generating a 10 Gb/s RZ modulated optical signal, that is transported by up to 10 km upstream fiber (ITU-T G.652) to a redistribution hub (see Figure 1(a)). Upstream traffic from all ONUs are merged by a 128×1 splitter and then again redistributed by another splitter 1×128 that channels back merged traffic to each ONU through a downstream fiber identical and parallel to the upstream one. Splitters' attenuation ($\simeq 25$ dB, estimated) contribute, as well as fiber attenuation ($\simeq 2$ dB each stretch) and insertion losses ($\simeq 1$ dB), to a high total round trip attenuation ($\simeq 55$ dB). In order to make the system workable it is proposed to place a single EDFA optical amplifier (≥ 27 dB gain) between both splitters. This EDFA will rise merged traffic power at first splitter output ($\simeq -25.5$ dBm for '1' active Tx) delivering enough power (-26 dBm, for '1' active Tx) at second splitter input to assure proper reception by a high sensitivity APD (-28 dBm) at each ONU.

3 Numerical simulations

We developed a modular simulator platform, where each block performs a single operation and they are totally interchangeable. For performance, each block including bloom-filter, error correction algorithms and the physical optical channel simulation were implemented in C++ and were released under the GNU license [7].

The physical optical channel simulation block was made to estimate bit error rate occurring in the optical channel. Traffic starts at a ONU's Tx that generates upstream traffic as an RZ optical signal. As a simplification it is assumed that traffic coming from all ONUs arrive at 1×128 splitter with perfect time synchronization (no jitter). This allows to simulate traffic merging at 128×1 splitter as a simple addition of optical intensities at each bit slot. Each bit slot coming from an ONU represents either a '0' or '1' bit. Bit '0' slots are represented by a flat signal given by Tx extinction ratio (a standard value of 10 dB was assumed for the simulation). As many bit '0' optical intensities are added as ONUs are assumed present (from 0

to 128). Bit '1' slots represent the optical signal amplitude of a super-Gaussian ($m = 4$) pulse with rising edge at slot start, with a peak amplitude that corresponds to Tx optical output power (2 dBm) adjusted by the pulse duty cycle (1/3). As many bit '1' intensities are added at each simulation bit slot as active Tx accordingly to this block's input file. Merged traffic reaches the EDFA after traversing 10 km fiber, 128×1 splitter and connectors/splices, so it's attenuated 27.5 dB.

Even as real EDFAs gain decreases with higher input power, as simplification it was simulated as a single gain for 27 dB gain for any number of active Txs. Noise produced by the EDFA is assumed to be white Gaussian noise. Traffic is routed back to all ONUs by a 1×128 splitter through another 10 km fiber, amounting to a 27.5 dB attenuation; so for one active Tx input power at each Rx is -26 dBm.

The optical signal arriving to each Rx is filtered with an optical filter (2nd order low pass Butterworth IIR filter,cutoff frequency 25 GHz), and then photodetected. Then electrical filtering is applied (i.e. optical). To account for thermal and shot noise at a typical APD white Gaussian noise current is added, with an estimated SNR $\simeq$ 42 dB (see section 4.4.3 at [1]). Decision circuit simulation compares a single sampling at each bit slot to a current threshold. This threshold was previously established at the time of maximum eye opening in a simulation performed with the same number of ONUs but with a single active Tx.

4 Simulation results

Figure 2(a) shows simulation results for the BER vs OSNR for different numbers of ONUs with fixed electrical SNR $\simeq$ 42 dB. Higher BERs as ONUs number increases due to the higher probability of simultaneous bit '1' transmissions (collisions) yielding pulses of optical power higher than that of a logical '1', generating intersymbol interference. Higher powers generate higher currents at Rxs that demand longer times to settle to logical '0' levels after filtering. Nevertheless, as can be seen in Figure 2(a), in the worst case scenario (128 ONUs) the expected OSNR at the EDFA output is enough ($\geq$ 40 dB) to ensure a BER$< 10^{-7}$. In this case simulation shown that the occurrence of 15 simultaneously active Tx was a very rare event, so optical power at Rx would be $\simeq -15$ dBm, well bellow standard commercial Rx overload of ~ 0.5 dBm (maximum acceptable mean input power for a BER$< 10^{-12}$).

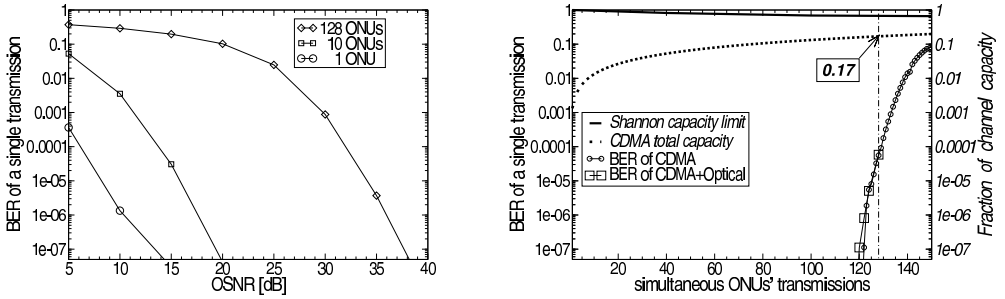
Figure 2(b) shows simulation results, where the fraction of the total capacity and BER of one channel at the access layer alone (circles) and both layers (squares). These results were obtained sending a 1 Gigabit of data for each ONU simultaneously.

Taking into account that the system was designed to support asynchronous communications (e.g., Ethernet), it is not likely that all the ONUs will transmit at the same time (e.g., Internet's links often operate at most at 90% load); and therefore our system has a BER $< 10^{-9}$ for each channel when 119 ONUs are transmitting at a same time ($119/128 > 0.9$). There is a very low penalty due the optical layer for low BER situations.

It is worth to remark that, even if the optical channel can induce a significant number of errors, the access layer has shown to be able to correct a very large number of errors (it is based on LDPC+ReedSolomon+ +BloomFilters), as can be seen on the curve with squares at Figure 2(b). The high bit error rates obtained in the simulation correspond to the worst-case, when all ONUs are transmitting at full capacity.

5 Conclusions

We demonstrated an OCDMA network able to connect 128 ONUs with enhanced security, despite some inherent inefficiencies of the selected algorithms. The proposed system has a lower communication rate than similar PON schemes but privacy is greatly increased and private networks between ONUs can be set up without additional high-level protocols. We also shown that the access layer is robust to high error rate coming from the physical layer. This opens the door to design a larger OCDMA network, covering larger distances and/or more ONUs. It seems possible to provide an adaptive and dynamic algorithm to use more capacity per channel to take advantage of the unused capacity.



(a) Optical channel (b) Logical channel

Fig. 2. Simulation results

Acknowledgement: This work was supported by grant PICT-497/2006 of the ANPCyT, Argentina.

References

[1] G. P. Agrawal. *Fiber-Optic Communication Systems*. John Wiley & Sons, Inc, 2002.

[2] B. H. Bloom. Space/Time Trade-offs in Hash Coding with Allowable Errors. *Communications of the ACM*, 13(7):422–426, 1970.

[3] A. Carena, V. De Feo, J. M. Finochietto, R. Gaudino, F. Neri, C. Piglione, and P. Poggiolini. RingO: an experimental WDM optical packet network for metro applications. *IEEE Journal on Selected Areas in Communications*, 22(8):1561–1571, 2004.

[4] S. W. Golomb. The limiting behavior of the Z-channel. *IEEE Transactions on Information Theory*, 26(3):372–372, 1980.

[5] W. Meier and O. Staffelbach. The Self-Shrinking Generator. In A. De Santis, editor, *Advances in Cryptology- EUROCRYPT'94*, pages 205–214. Springer, Berlin, 1994.

[6] T. K. Moon. *Error Correction Coding*. Wiley, 2005.

[7] A. A. Ortega, V. A. Bettachini, and J. I. Alvarez-Hamelin. ECC-chain simulator: `http://code.google.com/p/eccchain/`, 2008.

[8] L. G. Tallini, S. Al-Bassam, and B. Bose. On the capacity and codes for the Z-channel. In *IEEE Internation Symposium on Information theroy*, pages 422–422, 2002.