HAL
archives-ouvertes.fr

Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security

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

▶ **To cite this version:**

Ortega A. Alfredo, Victor A. Bettachini, José Ignacio Alvarez-Hamelin, Diego F. Grosz. Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security. 2009. <inria-00443517v3>

HAL Id: inria-00443517
https://hal.inria.fr/inria-00443517v3

Submitted on 3 Feb 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security

Alfredo A. Ortega, Víctor A. Bettachini, *
José Ignacio Alvarez-Hamelin and Diego F. Grosz,†

February 3, 2011

Abstract

We propose a network implementation with enhanced security at the physical layer by means of time-hopping CDMA, supporting cryptographically secure point-to-point and point-to-multipoint communication. In particular, we analyze an active star topology optical network implementation capable of supporting 128 simultaneous users up to 20 km apart. The feasibility of the proposed scheme is demonstrated through numerical simulation. **keywords:** *optical fiber communication, access networks, secure communication, CDMA*

1 Introduction

Communication methods employed today in access optical networks are inherently insecure, as they do not provide privacy from a sufficiently motivated eavesdropper, as signals are broadcasted to all users, e.g., as in Passive Optical Networks (PONs). Communication security must be implemented by the end-points on higher-level protocols, and is often neglected.

This paper proposes an access network architecture where security is provided by a time-hopping CDMA scheme at the physical layer. The proposed scheme provides point-to-point and point-to-multipoint communication, allowing the setup of Virtual Private Networks (VPNs) among users. In this way, each client transmits in frame slots assigned by a cryptographically secure PRBS. Since each user transmits one bit per slot, collisions occur and are handled by a combination of Bloom filters [2] and standard error-correction algorithms optimized for Z channels [6]. Bloom filtering is a technique borrowed from hashing algorithms where a bit is transmitted in K slots into the same frame; therefore

*A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, and D. F. Grosz are with Instituto Tecnológico de Buenos Aires, 25 de Mayo 444, C1002ABJ, Buenos Aires, Argentina (e-mail: aortega@alu.itba.edu.ar, {vbettachini,ihameli,dgrosz}@itba.edu.ar).

†J. I. Alvarez-Hamelin, and D. F. Grosz are also with CONICET (Argentine Council of Scientific and Technological Research).

it is sufficient to receive a single '0' out of K copies in order to correctly retrieve the original transmitted '0' whereas, in a Z channel, collisions have no effect on '1s'.

An early approach to this idea was presented in [14], where a combination of wavelength hopping and direct sequence CDMA with orthogonal codes was used to provide security in the link, whereas our proposal uses a single wavelength and time hopping CDMA. More recently, Refs. [9] and [10] proposed a VPN built with direct sequence CDMA using Walsh orthogonal coding on a single wavelength channel. Although orthogonal codes make an efficient use of the available bandwidth, in Ref. [12] it is shown that the security they provide is weak due to the reduced code space. Finally, Ref. [15] used the Advanced Encryption Standard (AES) to encrypt data, and then sent this encoded stream by direct sequence CDMA with a short code length, that is, security is provided in a higher layer, i.e., as is standard cryptography [12]. In contrast, our proposed scheme uses a *key* to feed each PRBS giving non-orthogonal coding sequences, thus producing a larger search space in case an attack is attempted. Moreover we use a non-linear generator, e.g., a self-shrinking generator [7].

The architecture proposed in this paper consists of a star network topology using a single wavelength, in contrast to other optical access network designs [3]. The proposed topology and functionality resemble that of a PON (users can be regarded as Optical Network Units, ONUs) but note that point-to-point as well as point-to-multipoint communication are supported. To receive an specific channel, the user/ONU needs the corresponding *key*, thus it can communicate as many users as *keys* it has. A privileged user can communicate all other users acting as the Optical Line Termination (OLT) in PONs.

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. The access layer is implemented using time-hopping CDMA, where each of the 128 possible ONUs sends bits in a slot randomly chosen from a frame of 356 slots; therefore collisions between different ONUs will occur and error correction must be used to guarantee error-free transmission. Notice that the synchronization is performed at the bit slot level only because transmission of each ONU is random, in contrast to TDMA where synchronization is also performed at the frame level. Moreover, each ONU can send data at any time, in contrast to TDMA where ONUs usually send data continuously; this feature resembles transport by Ethernet frames. A certain ONU X can receive messages from an ONU Y if X has the *key* of Y, and viceversa. Therefore, if a certain group of ONUs were to communicate over a VLAN, it is required that everyone in the group knows each others' *keys*. ONUs' data streams are encoded with the following error correction techniques (Fig. 1): Reed-Solomon (223/255) and LDPC (1024×512 matrix) algorithms (see [8] and references therein), and Bloom-filters with $K = 4$ [2]. The choice of these

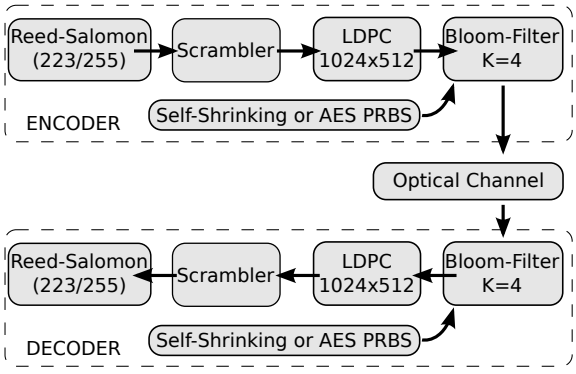

Figure 1: Proposed network design: Access Layer

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 [13].

The proposed physical layer topology is that of a star (see Fig. 2) where optical splitters redistribute traffic coming from each ONU to all the rest allowing point-to-multipoint as well as point-to-point communications between 128 ONUs. An Erbium-Doped Fiber Amplifier (EDFA) located in between splitters at the optical hub increases optical power to overcome network losses. RZ modulated optical signals generated at each ONU, of up to 10 Gbps by a 2 dBm 1550 nm DFB-laser, are transmitted up to 10 km upstream by a standard single-mode optical fiber (ITU-T G.652) to the optical hub.

In this hub a 128×1 splitter merges traffic from all ONUs that is then redistributed by a 1×128 splitter channeling back merged traffic to each ONU through a downstream fiber identical and parallel to the upstream fiber. Splitters' attenuation ($\simeq$ 25 dB each) contribute, as well as fiber attenuation and insertion losses ($\simeq$ 2 dB and $\simeq$ 1 dB per stretch), to high total losses ($\simeq$ 28 dB at both upstream and downstream paths). In order to provide signal amplification an EDFA ($\geq$ 27 dB gain and noise figure 7 dB) is placed between both splitters. This EDFA increases merged traffic power at the first splitter output ($\simeq -26$ dBm '1' active Tx) delivering an adequate power level (1 dBm, '1' active Tx) at the second splitter input to provide ONU's receiver a power level for proper reception (-27 dBm, '1' active Tx) with a high sensitivity (-28 dBm) photodetector (PD). The PD maximum optical power is not a concern as our simulations show that only up to ten '1s' collide at any given bit slot. Even considering a constant EDFA gain, the PD input optical power would be lower (-17 dBm) than that commercial PDs withstand unharmed (~ -5 dBm). The bit '0' level at PD is given by the addition of the '0' bit transmitted by all 128 ONUs. The receiver decision threshold should be able to separate between this state and that of a single ONU transmitting a '1' bit. As the bit '0' trans-

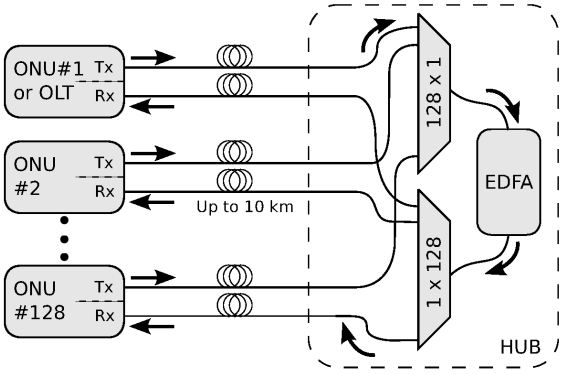

Figure 2: Proposed network design: Optical Layer

mission power should be very low, imposing restrictions on the DFB-laser extinction ratio. The minimal required extinction ratio ('1'/'0' peak power ratio) is addressed in the numerical simulations explained next.

3 Numerical simulations

We developed a modular simulator platform both for ECC and optical channel stages. It was released under the GNU license [11].

The physical optical channel simulation block provides an estimate of the BER performance of the optical channel. Simulation steps are as follows: RZ upstream traffic coming from all ONUs is assumed to arrive at the 128×1 splitter with perfect time synchronization, i.e., there is no timing jitter. The '0'-bit slots contain a small CW optical intensity given by the Tx extinction ratio. Each on-line ONU adds its '0'-bit optical intensity yielding a base power level. Each '1'-bit adds a super-Gaussian ($m = 4$) pulse, duty cycle 1/3, to the base power level.

Upstream and downstream merged traffic suffers from attenuation due to splitter, fiber, and splice losses. The power budget is balanced by an EDFA with 27 dB constant gain. Amplified spontaneous emission from the EDFA is modeled by white Gaussian noise, with intensity proportional to the amplifier noise figure (7 dB), and is added after the EDFA.

The input optical signal at the receiver is filtered (2nd order low-pass Butterworth filter, 25 GHz bandwidth) and photodetected assuming a standard PD responsivity (see section 4.4.3 of [1]). White Gaussian noise accounting for thermal and shot noise is then added to the photocurrent, and electrical filtering is applied (2nd order low-pass Butterworth filter, 14 GHz bandwidth).

Noise fluctuations at power levels near the PD sensitivity limit have an important effect on signal detection. Shot noise is of particular concern as it is proportional to the mean photocurrent. In our network proposal the later is

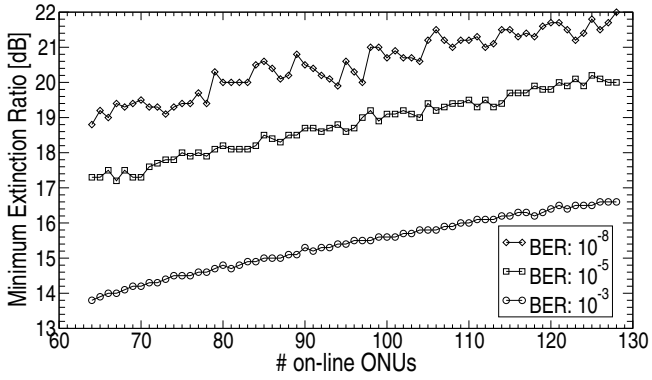

Figure 3: Physical (optical) layer simulation result: Minimal extinction ratio required to assure a given BER.

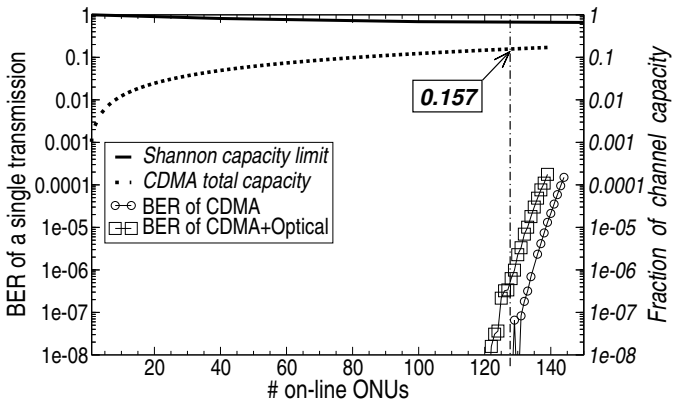

Figure 4: Simulation results: Logical channel

higher than in PONs as bit '0' optical intensities from all ONUs are added. The resulting base-level optical intensity is then heavily dependent on the Tx extinction ratio. Fig. 3 shows minimal extinction ratios required to achieve an arbitrary BER in the physical layer as a function of the number of on-line ONUs. In the 128 ONUs scenario a BER$< 10^{-3}$ can be achieved using commercially available transmitters with an extinction ratio $\simeq$ 16.6 dB. This BER is low enough to allow for logical-channel error-correction routines that guarantee error-free transmission, while still making use of a fair fraction of channel capacity when non-orthogonal codes are used. Fig. 4 shows simulation results for the fraction of the total capacity and the BER of one channel at the coding level (circles) and including physical layer impairments (squares). These results were obtained by sending one Gigabit of data for each ONU simultaneously. This figure shows a channel utilization of 15.7% when all of 128 ONUs are transmit-

ting simultaneously, with a BER$< 10^{-8}$. From Fig. 2 we observe a penalty of 8 ONUs when impairments from the optical layer (mainly extinction ratio and noise from EDFA and PDs) are taken into account. Considering that the system was designed to support asynchronous communications (e.g., Ethernet), it is not likely that all the ONUs will transmit simultaneously (e.g., Internet links often operate at most at 90% load); and therefore our system has a BER $< 10^{-8}$ for each channel when 119 ONUs are transmitting at a same time ($119/128 > 0.9$). Observe that the high error rates correspond to a worst-case scenario when all ONUs are transmitting simultaneously at full capacity, and also there is a low penalty due to physical layer impairments.

4 Security Performance

There are four basic goals related to security performance: Confidentiality, integrity, availability and authenticity [5]. The proposed scheme provides confidentiality and integrity in the downstream channel, leaving availability and authenticity implementations to higher-level protocols. Confidentiality and integrity are achieved by using time-hopping CDMA. Attacks on this kind of systems are extensively studied in [12]. The proposed system is resistant to brute-force attacks since the code space size can be grater than 2^{256} (related to the period of the PRBS), the proposed PRBS is non-linear e.g., a self-shrinking generator [7] or AES in PRBS mode, and the key of each ONU is never broadcasted to the network. The key distribution must be performed beforehand using any secure method available [4]

5 Conclusions

We proposed a time-hopping CDMA network architecture capable of supporting both point-to-point and point-to-multipoint communication of up to 128 ONUs with a worst-case rate of 12 Mbps. Furthermore, the proposed scheme provides security at the physical layer and VPNs between ONUs can be set up without additional higher-level protocols. We also showed that there is a low penalty due to physical layer impairments, such as transmitter extinction ratio and attenuation at fibers, splitter, and splices. We believe that our proposal opens the door to the design of a larger secure CDMA network, covering longer distances and servicing more end users.

Acknowledgment

This work was supported by grant PICT-497/2006 ANPCyT Argentina, and also by Core Security Technologies.

References

[1] G. P. Agrawal. *Fiber-Optic Communication Systems*. John Wiley & Sons, New York, USA, second edition, 1997.

[2] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, 13(7):422–426, July 1970.

[3] A. Carena, V. D. Feo, J. M. Finochietto, R. Gaudino, F. Neri, C. Piglione, and P. Poggiolini. Ringo: An experimental wdm optical packet network for metro applications. *IEEE J. Sel. Areas Commun.*, 22(8):1561–1571, October 2004.

[4] D. E. R. Denning. *Cryptograghy and Data Security*. Addison-Wesley Publishing Company, Inc., Reading MA., USA, 1982.

[5] Gurpreet Dhillon. *Principles of Information Systems Security: text and cases*. John Wiley & Sons, New York, USA, 2007.

[6] S. W. Golomb. The limiting behavior of the z-channel. *IEEE Trans. Inf. Theory*, IT-26:372, May 1980.

[7] 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.

[8] T. K. Moon. *Error Correction Coding: Mathematical Methods and Algorithms*. John Wiley & Sons, New York, USA, 2005.

[9] N. Nadarajah, E. Wong, and a. Nirmalathas. Implementation of multiple secure virtual private networks over passive optical networks using electronic CDMA. *IEEE Photonics Technology Letters*, 18(3):484–486, February 2006.

[10] Ampalavanapillai Nirmalathas, Nishaanthan Nadarajah, and Elaine Wong. Multiple secure virtual private networks over passive optical networks using electronic CDMA. *2009 IEEE/LEOS Summer Topical Meeting*, 1:13–14, July 2009.

[11] A. A. Ortega, V. A. Bettachini, and J. I. Alvarez-Hamelin. Ecc-chain simulator, 2008.

[12] T.H. Shake. Security performance of optical cdma against eavesdropping. *J. Lightw. Technol.*, 23:655–670, February 2005.

[13] L. G. Tallini, S. Al-Bassam, and B. Bose. On the capacity and codes for the z-channel. In *Proc. IEEE International Symposium on Information Theory (ISIT'02)*, page 422, Lausanne, Switzerland, June 2002.

[14] L. Tancevski, I. Andonovic, and J. Budin. Secure optical network architectures utilizing wavelength hopping/time spreading codes. *J. Lightw. Technol.*, 7:1041–1135, May 1995.

[15] Z. Wang, L. Xu, J. Chang, T. Wang, and P. R. Prucnal. Secure optical transmission in a point-to-point link with encrypted cdma codes. *Photonics Technology Letters, IEEE*, 22(19):1410 –1412, oct. 2010.