Sistema de transmisión segura punto a punto y multipunto en medios compartidos.

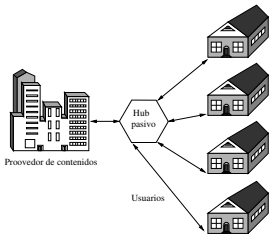
Alfredo Adrián Ortega
Instituto Tecnológico de Buenos Aires (ITBA)
aortega@alu.itba.edu.ar

24 de noviembre de 2015

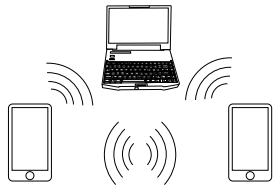
Contenido

Introducción

- Tema: Seguridad en redes de acceso ópticas.
  - Comunicaciones seguras utilizando CDMA sobre fibra óptica.
  - Velocidades de 5 GBPS o mas.
- Subtema: Comunicaciones acústicas privadas.



(a) Red óptica



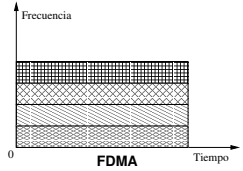
(b) Red acústica

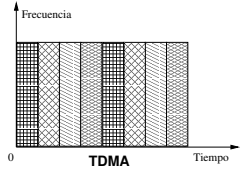
Problemas a resolver

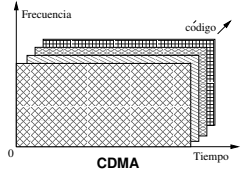
- Privacidad de datos en una red que utiliza un medio compartido
- Protección ante nodos maliciosos
- Eliminar toda fuga de información

Solucion propuesta

1. Utilizar CDMA para la separación en canales
2. Desarrollar algoritmos criptográficamente seguros para la privacidad







Desafíos

1. Sistema capaz de operar a 5 Gbps+
2. Evitar protocolos de control que debiliten la criptografía
3. Aislación completa de canales de comunicación, para evitar ataques del tipo side-channel.
4. Alta performance y bajo costo

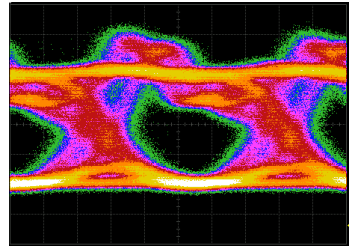
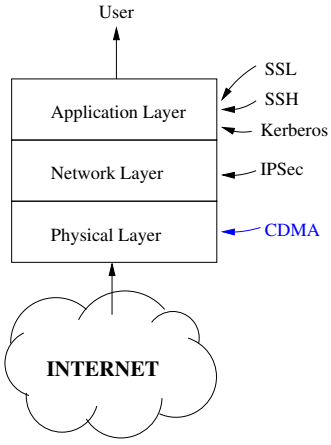


Figura : Diagramas de ojo, tasa de 7,5 Gbps, 20ns por división.

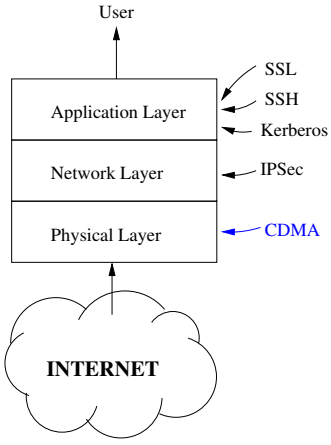
Seguridad en las capas de red



Modelo de red OSI simplificado

- SSH
- SSL
- Kerberos

Seguridad en las capas de red



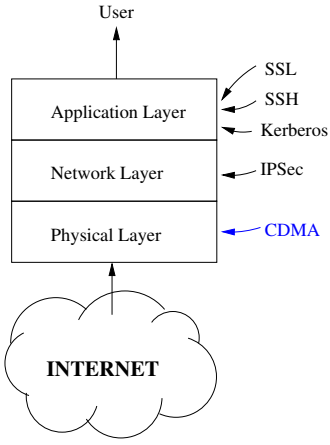
Modelo de red OSI simplificado

- SSH
- SSL
- Kerberos

Desventajas:

- Usualmente mal configurada
- Directamente olvidada

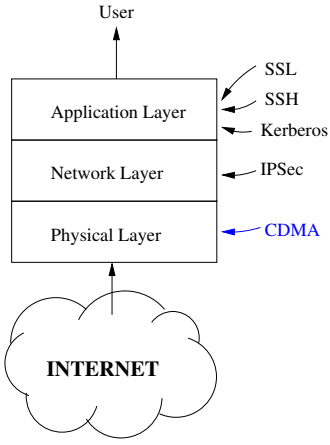
Seguridad en las capas de red



Modelo de red OSI simplificado

- Reflectores de tipo rejilla de Bragg (*Bragg Grating*) [Torres et al.(2002)]
  - Configuración Fija

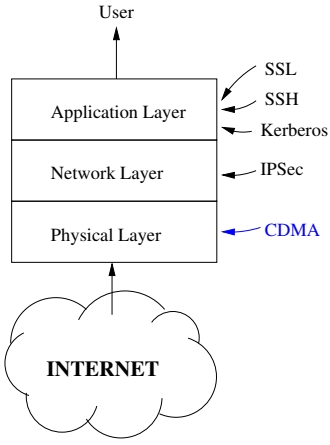
Seguridad en las capas de red



Modelo de red OSI simplificado

- Reflectores de tipo rejilla de Bragg (*Bragg Grating*) [Torres et al.(2002)]
  - Configuración Fija
- Sistema propuesto en [Mosso et al.(2011)]
  - Baja cantidad de canales (crosstalk)
  - Espacio de claves reducido

Seguridad en las capas de red



Modelo de red OSI simplificado

- Reflectores de tipo rejilla de Bragg (*Bragg Grating*) [Torres et al.(2002)]
  - Configuración Fija
- Sistema propuesto en [Mosso et al.(2011)]
  - Baja cantidad de canales (crosstalk)
  - Espacio de claves reducido
- CDMA & códigos Walsh [Nadarajah et al.(2006)]
  - Espacio de claves muy reducido [Shake(2005)]

Sistema propuesto

Basado en:

Time-hopping CDMA: El tiempo de transmisión se selecciona mediante un algoritmo generador de números pseudoaleatorios (PRBS).

Filtro de Bloom: Provee corrección de errores asimétrica (en un canal Z)

Minimización de peso de Hamming: reducción de símbolos problemáticos en el canal Z

Sistema propuesto

Basado en:

Time-hopping CDMA: El tiempo de transmisión se selecciona mediante un algoritmo generador de números pseudoaleatorios (PRBS).

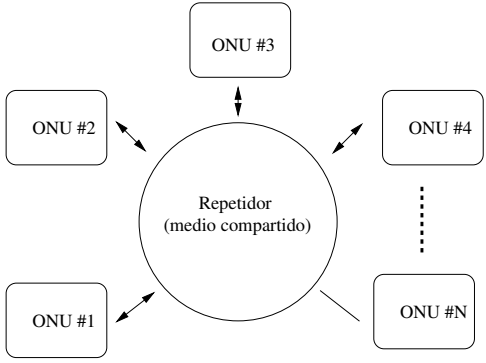
Filtro de Bloom: Provee corrección de errores asimétrica (en un canal Z)

Minimización de peso de Hamming: reducción de símbolos problemáticos en el canal Z

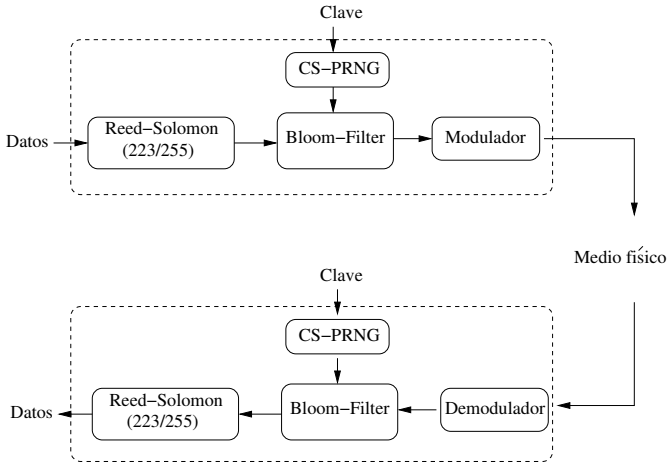
Ventajas:

- Punto-a-punto y Punto-a-Multipunto
- Privacidad

Sistema propuesto: diseño de alto nivel



Sistema propuesto: diagrama esquemático



Canal Z

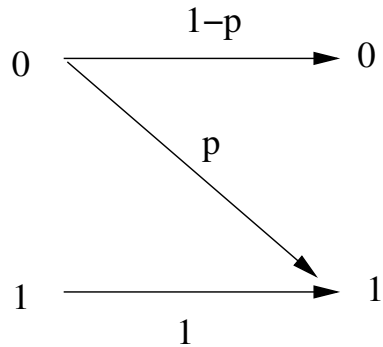
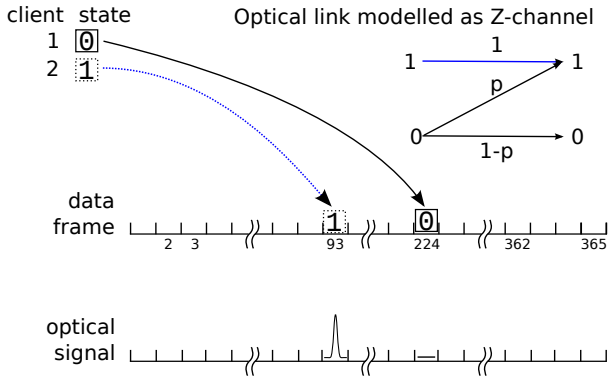


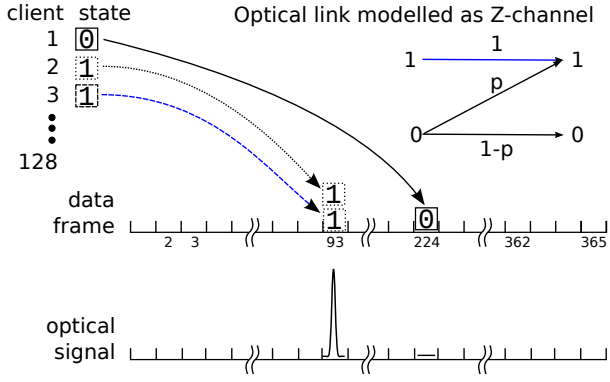
Figura : Diagrama de probabilidad del un canal binario asimétrico o canal Z

Selección de casillero aleatoria: Time hopping



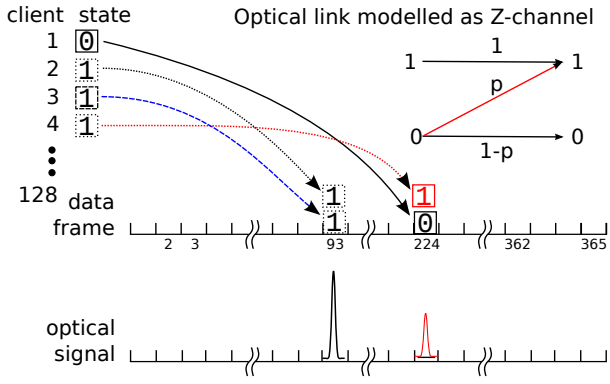
No hay colisión

Selección de casillero aleatoria: Time hopping



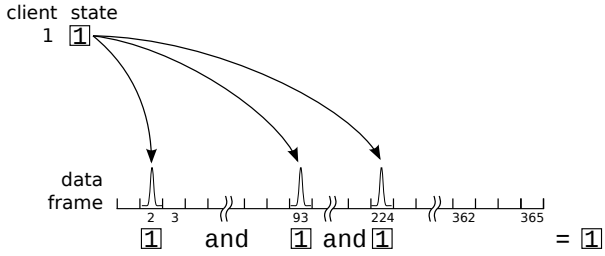
Colisión $\Rightarrow$ Resultado OK

Selección de casillero aleatoria: Time hopping



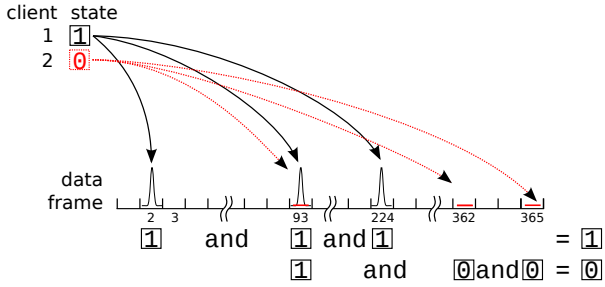
Colisión $\Rightarrow$ Error

CDMA + Filtro de Bloom (K=3)



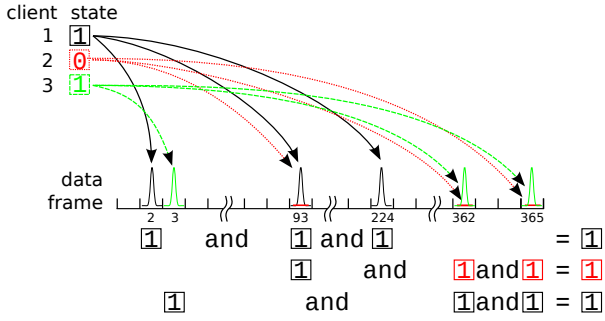
Inserta el bit '1' en la trama

CDMA + Bloom filter (K=3)



Inserta el bit '0' en la trama

CDMA + Bloom filter (K=3)



Inserta el bit '1' en la trama $\Rightarrow$ Error

K Óptimo

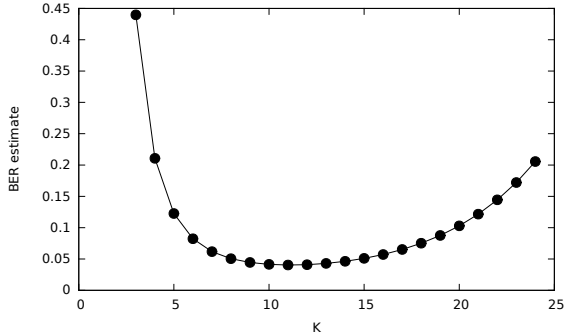


Figura : Estimación de BER vs. tasa de repetición de filtro de Bloom K.

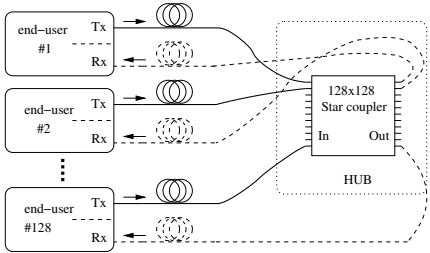
$$\text{BER} \approx \frac{n}{2} m_0 z_{\bar{R},\bar{S}} \approx \frac{n}{2} m_0 \left(1 - e^{-W_1/M}\right)^K. \quad (1)$$

Minimización de peso de Hamming

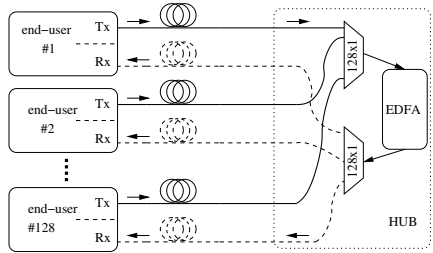
Símbolo de 3-bits, Peso de Hamming=2, expansión a 5 bits

Dato	Entrada, HW=variable	Expansión HW=2
0	000	00011
1	001	00110
2	010	00101
3	011	01100
4	100	01010
5	101	01001
6	110	10001
7	111	10010

Implementación: Fibra Óptica



(a) Distribución via acoplador tipo estrella 1

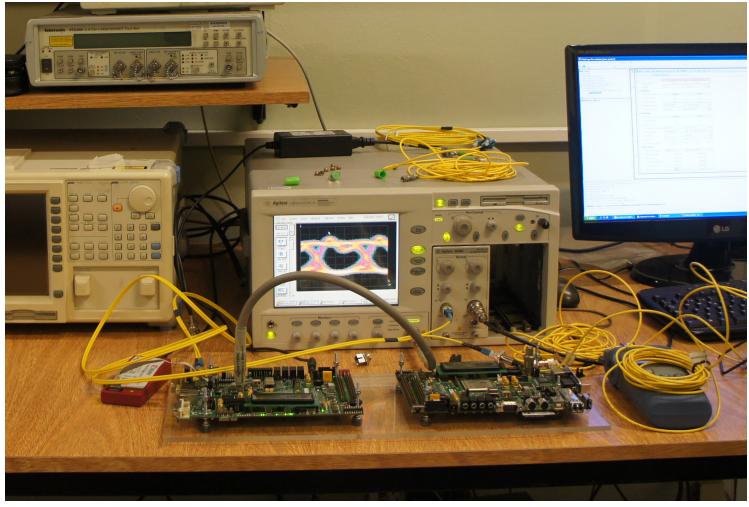


(b) Distribución via EDFA

Figura : Diseño de red propuesto para la capa óptica

Implementación: Fibra Óptica

Placas de desarrollo Xilinx ML507



Implementación: Fibra Óptica

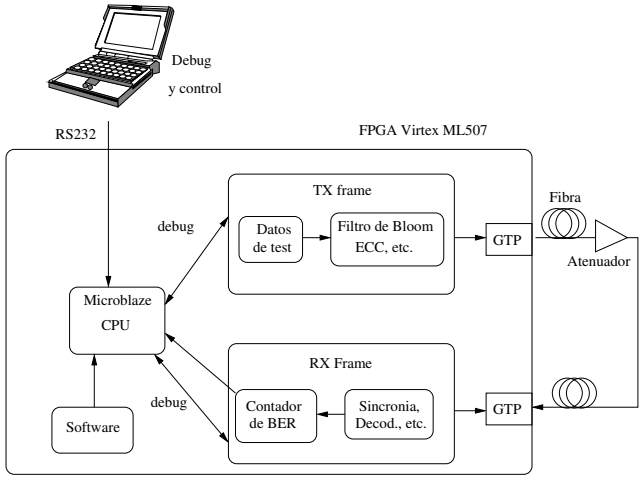
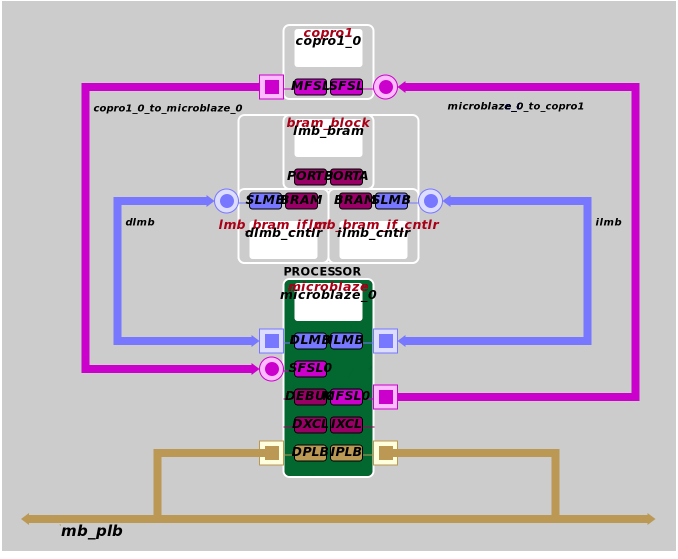


Figura : Diseño lógico de alto nivel sobre FPGA

Implementación: Fibra Óptica, FPGA



Implementación: Fibra Óptica, Resultados (Simulaciones)

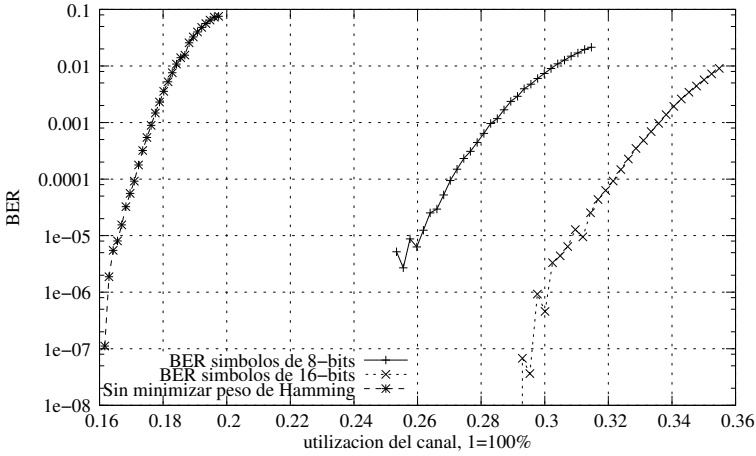
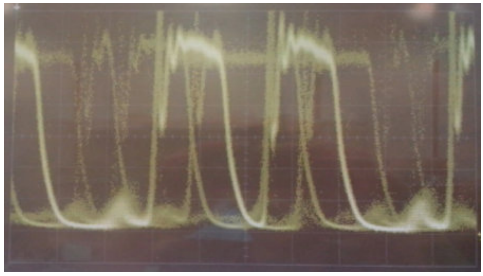
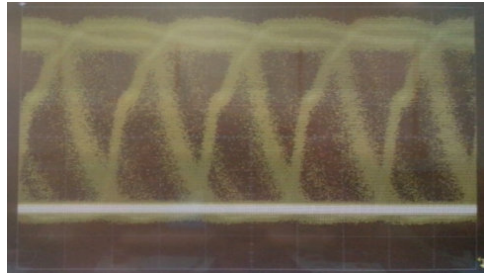


Figura : Performance del sistema con respecto a la expansión de símbolo. Simulación numérica de un enlace de 10 Gbps con 128 clientes, M=4096 y K=9.

Implementación: Efectos de señal desbalanceada



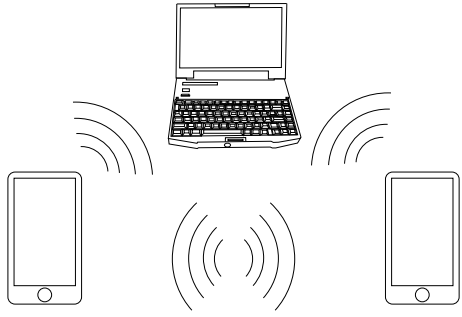
(a) Señal con 256 bits en uno por trama (8B/10B), 400 ps por bit



(b) Señal con 48 bits en uno por trama, 1100 ps por bit

Figura : Señal de potencia óptica de un Láser SPF+ Sumitomo de 1330 nm, tasa nominal es de 2.5 Gbps

Medio acústico: Introducción



Esquema de transmisión acústica

- Originalmente plataforma de testing del medio óptico
- Fácil de depurar e implementar (100 % software)
- Equivalente a un módem por software

Medio acústico: Modulación

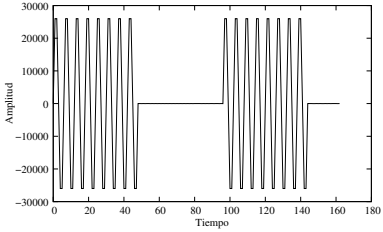


Figura : Modulación OOK

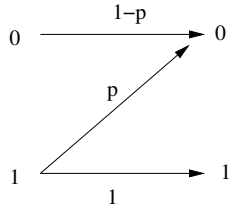
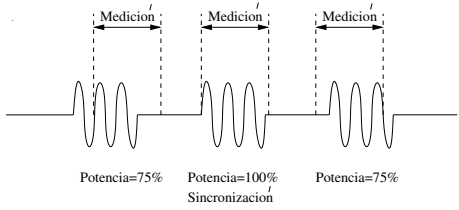


Figura : Diagrama de probabilidad: canal Z

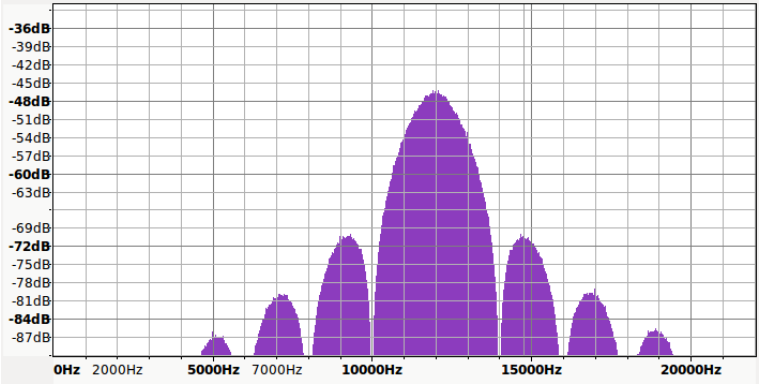
- Interferencia de OOK se aproxima a la de un canal Z.
- Baja densidad espectral ($0{,}2 bits/s/Hz$)

Medio acústico: Sincronización



Sincronización de bit/nivel de decisión

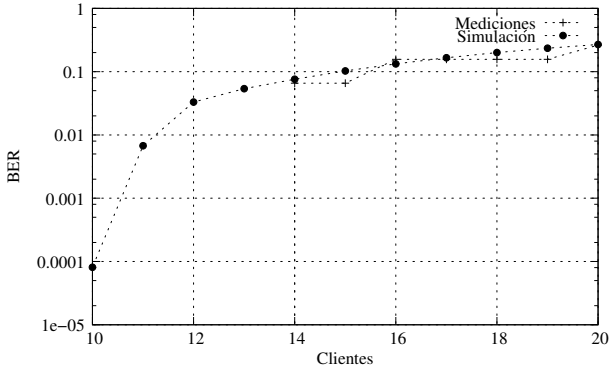
Medio acústico: Características y espectro



Espectro de señal modulada

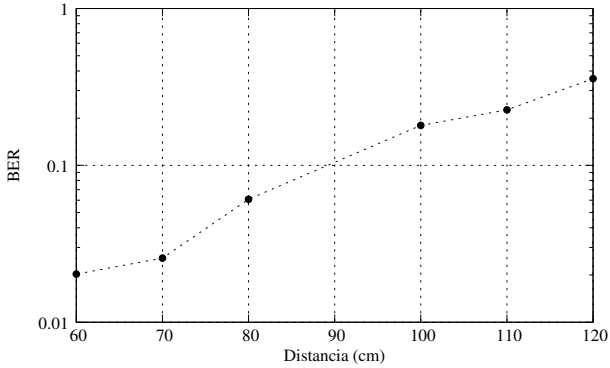
- Portadora a 12Khz, modem funcionando a 1Kbps en total
- Velocidades de 350 bps (2 usuarios) a 70 bps (10 usuarios)
- Dispositivos móviles: buen desempeño Parlante/Micrófono de 100 a 15Khz

Medio acústico: Resultados (mediciones)



BER *vs.* Clientes

Medio acústico: Resultados (mediciones)



BER *vs*. Distancia

Conclusiónes:

- Se propuse una arquitectura de red de tipo time-hopping CDMA:

Conclusiónes:

- Se propuse una arquitectura de red de tipo time-hopping CDMA:
  - Punto-a-Punto, y Punto-a-Multipunto.

Conclusiónes:

- Se propuse una arquitectura de red de tipo time-hopping CDMA:
  - Punto-a-Punto, y Punto-a-Multipunto.
  - Red Privada y criptográficamente segura.

Conclusiónes:

- Se propuse una arquitectura de red de tipo time-hopping CDMA:
  - Punto-a-Punto, y Punto-a-Multipunto.
  - Red Privada y criptográficamente segura.
  - Utilizando Filtros de Bloom y minimización de peso de Hamming.

Conclusiónes:

- Se propuse una arquitectura de red de tipo time-hopping CDMA:
  - Punto-a-Punto, y Punto-a-Multipunto.
  - Red Privada y criptográficamente segura.
  - Utilizando Filtros de Bloom y minimización de peso de Hamming.
  - **29 % de utilización del canal.**

Contribuciones:

Altas velocidades de transferencia en fibra óptica utilizando FPGAs de bajo costo. *A. A. Ortega, V. A. Bettachini, D.F. Grosz, J. I. Alvarez-Hamelin - Congreso de Microelectrónica Aplicada 2010 BsAs*

Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security *A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, D.F. Grosz, Advanced Photonics 2011 Congress - Access Networks and In-house CommunicationsAccess Networks and In-house Communications, OSA Technical Digest, Optical Society of America*

Hamming-weight minimisation coding for CDMA optical access networks with enhanced security *A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, D.F. Grosz, Future Generation Communication Technology (FGCT), 2012*

Contribuciones:

Encrypted CDMA Audio Network. *A. A. Ortega, V. A. Bettachini, P. I. Fierens, y J. I. Alvarez-Hamelin - Journal of Information Security - 2014*

Patente: DISPOSITIVO Y MÉTODO PARA TRANSMISIÓN SEGURA DE DATOS SOBRE CANALES Z MEDIANTE CDMA (AR084155B1) *José Ignacio ALVAREZ HAMELIN, Victor Alexis BETTACHINI, and Alfredo ORTEGA. PCT, 12 2012. (Asignada)*

Patente: Device and Method for the Secure Transmission of Data over Z-Channels Using CDMA (P11104EPPC) *José Ignacio ALVAREZ HAMELIN, Victor Alexis BETTACHINI, and Alfredo ORTEGA. EPO, Julio 2014. (En trámite)*

J. Daemen and V. Rijmen.
Aes proposal: Rijndael, 1998.

F. Mosso, J. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba.
All-optical encrypted movie.
Opt. Express, 19(6):5706–5712, 2011.

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, Feb. 2006.
ISSN 1041-1135.
doi: 10.1109/LPT.2005.863637.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1576846.

A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, and D. F. Grosz.
Point-to-point and point-to-multipoint cdma access network with enhanced security.
In *Access Networks and In-house Communications, OSA Technical Digest (CD), paper ATuB6*, Toronto, Canada, June 2011.

T. Shake.
Security performance of optical cdma against eavesdropping.

IEEE Journal of Lightwave Technology, 23:655–670, Feb. 2005.


P. Torres, L. Valente, and M. Carvalho.
Security system for optical communication signals with fiber bragg gratings.
50:13–16, Jan. 2002.


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.
IEEE Photonics Technology Letters, 22(19):1410 –1412, oct. 2010.
ISSN 1041-1135.
doi: 10.1109/LPT.2010.2061223.