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

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

3 de diciembre de 2015

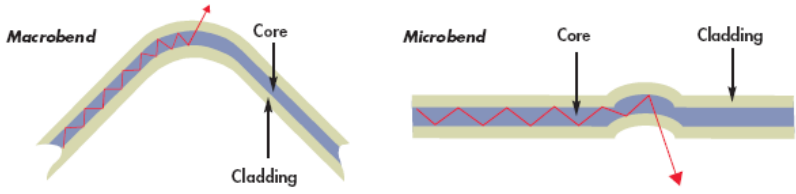
Contenido

Motivación

- Lograr privacidad a nivel físico en comunicaciones digitales.
- El costo de las intrusiones y robo de datos en el 2011 en EEUU ascendió en promedio a 5.5 us$ millones por organización (Symantec).
- Facilidad de robo de datos en medios compartidos.
- Productos comerciales (ID Quantique, NuCrypt, etc.) intentan solucionar este tipo de problemas.

Robo de datos en fibras ópticas

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



Fugas por Microbend y macrobend en fibra óptica [Jay, John A]

Robo de datos en fibras ópticas

Glimmerglass
Cyber Solutions

Home | Products | Solutions | Resources | News & Events | Company | Contact Us

Home » Products » -- Intelligent Optical Systems » -- Intelligent Optical System 500

Intelligent Optical System 500

Flexible: SDN and 100Gbps compatible

Scales from: 32x32 to 192x192

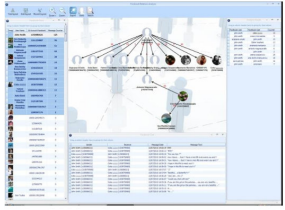
Overview: The Intelligent Optical System 500 is specifically designed for maximum flexibility of connector types and Telecom standard chassis depth. The System 500 allows for 192x192 fibers with either MTP or LC connectors. Our advanced user interface makes it easy to view and manage all connections.

Intelligent Optical System 500
Data Sheet

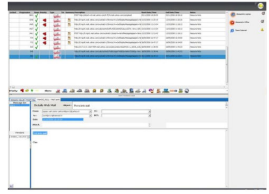
Robo de datos en fibras ópticas

Monitor Internet, Webmail, VoIP, Internet, Mobile

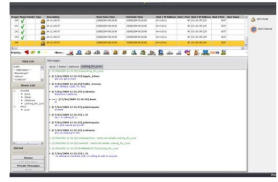
Facebook



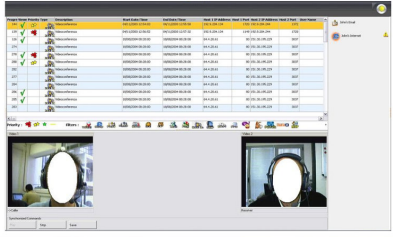
Webmail



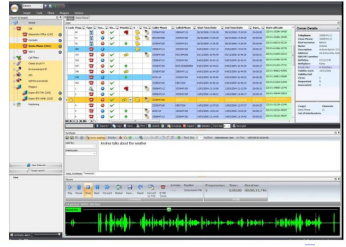
Chat



Internet Sessions: NetMeeting

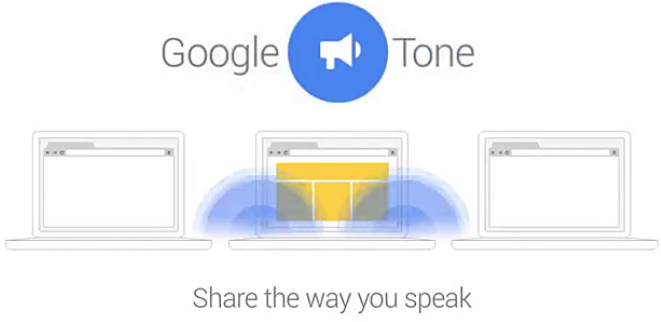


Wired / Wireless Phone Calls



Privacidad en redes acústicas

- Transmisión segura de claves/contacto/sistemas de TFA.
- Transacciones comerciales a corta distancia.
- Reemplazo de NFC, sin hardware específico.
- Ej. Google tone: *"An experimental chrome extension for instant sharing over audio"*

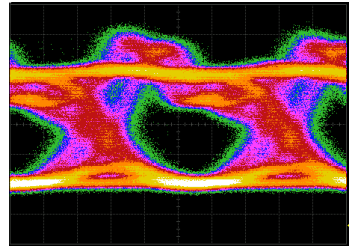


Red pública con privacidad

1. Red: enlaces punto-a-punto y multipunto.
2. Privacidad: nivel físico, criptográficamente fuerte.
3. CDMA: acceso asincrónico sin control centralizado.
4. Diferentes medios:
   - 4.1 Guiados: Fibra óptica
   - 4.2 No guiados: Electromagnético y acústico.

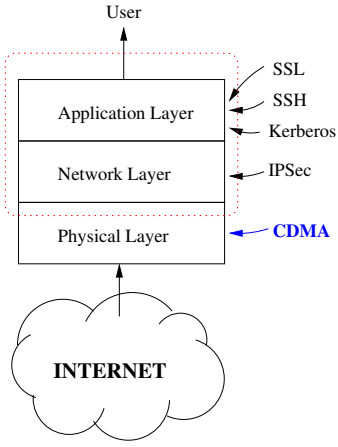
Desafíos en medios acústicos y fibra óptica

1. Evitar protocolos de control que debiliten la criptografía
2. Aislación completa de canales de comunicación, para evitar ataques del tipo *side channel*.
3. Bajo costo - utilización de hardware pre-existente.
4. Fibra óptica: Sistema capaz de operar a 5 Gbps+
5. Medio acústico: Bajo consumo de potencia y alta frecuencia de portadora.



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

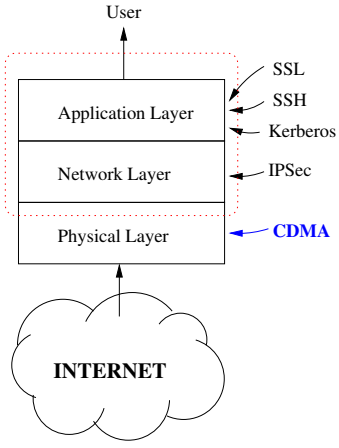
Seguridad en las capas de red



Modelo de red OSI simplificado

- SSH - solo punto-a-punto.
- SSL - protocolo muy complejo, muchas vulnerabilidades.
- IPSEC - poco difundido, configuración compleja
- Kerberos - idem SSL.

Seguridad en las capas de red



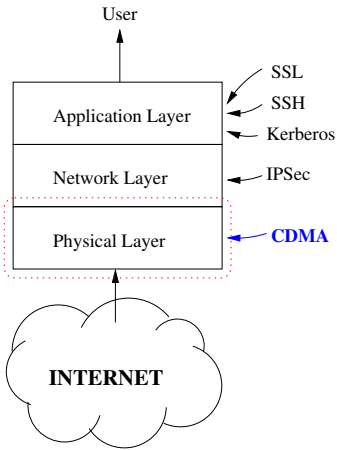
Modelo de red OSI simplificado

- SSH - solo punto-a-punto.
- SSL - protocolo muy complejo, muchas vulnerabilidades.
- IPSEC - poco difundido, configuración compleja
- Kerberos - idem SSL.

Desventajas:

- Complejidad y vulnerabilidades de implementación.
- Problemas en la configuración.

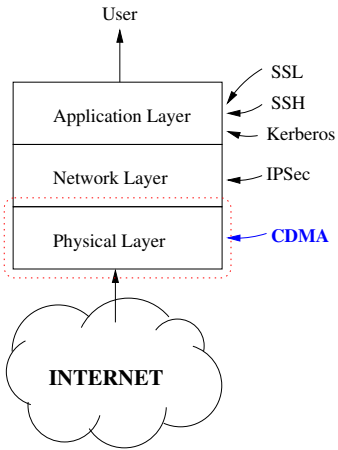
Seguridad en las capas de red



Modelo de red OSI simplificado

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

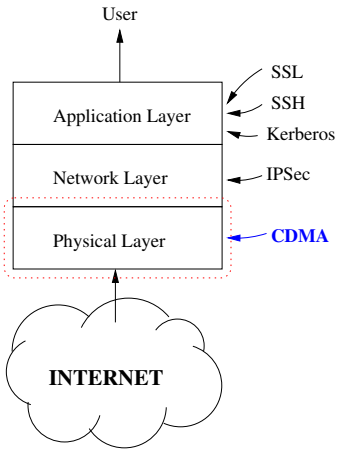
Seguridad en las capas de red



Modelo de red OSI simplificado

- Reflectores de tipo red 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 red 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-Hadamard [Nadarajah et al.(2006)]
  - Perfectamente ortogonales.
  - Espacio de claves muy reducido [Shake(2005)]

Sistema propuesto

Basado en:

- Medio de tipo bróadcast, modelado como canal Z
- Utilización de CDMA
- Corrección de errores optimizada para el tipo de canal

Sistema propuesto

Basado en:

- Medio de tipo bróadcast, modelado como canal Z
- Utilización de CDMA
- Corrección de errores optimizada para el tipo de canal

Ventajas:

- Punto-a-punto y Punto-a-multipunto
- Privacidad

Canal Z

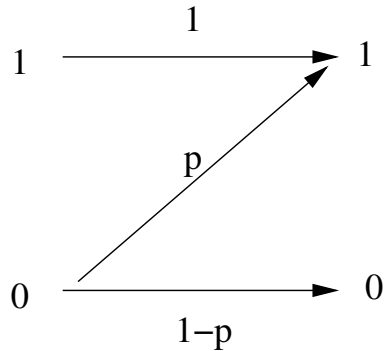
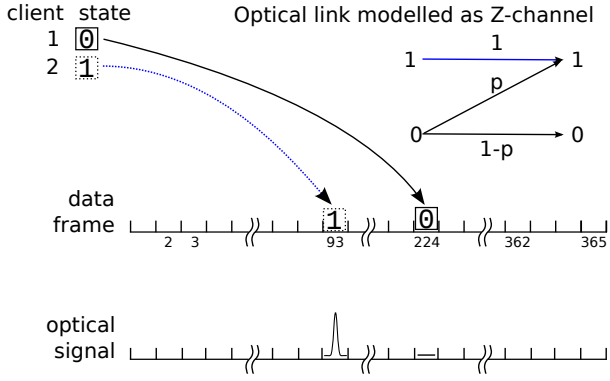


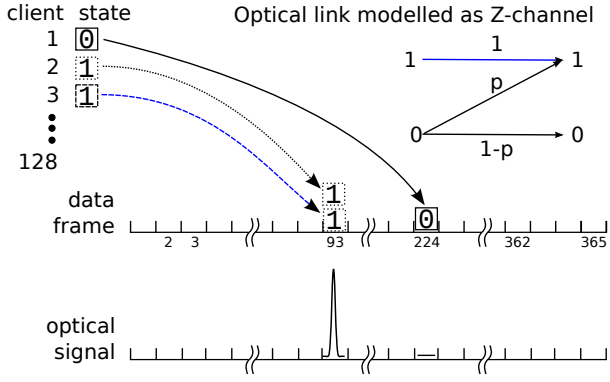
Diagrama de probabilidad del canal binario asimétrico o canal Z, donde p es la probabilidad de error.

Selección de casillero aleatoria: *time hopping*



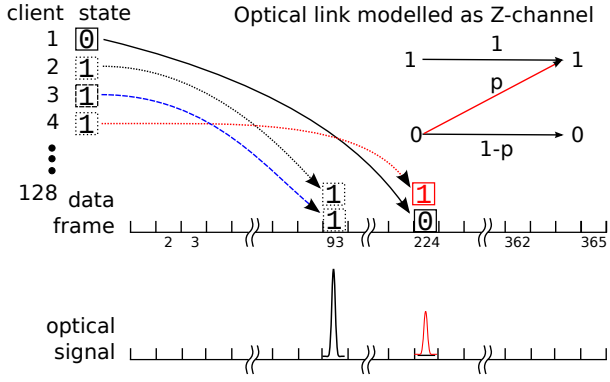
No hay colisión

Selección de casillero aleatoria: *time hopping*



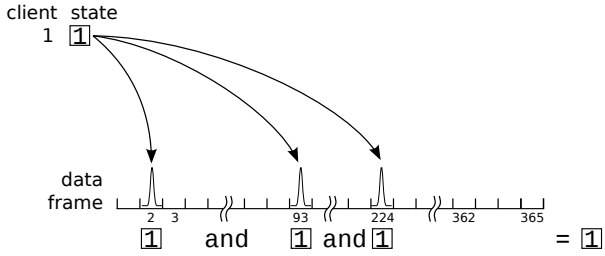
Colisión $\Rightarrow$ Resultado OK

Selección de casillero aleatoria: *time hopping*



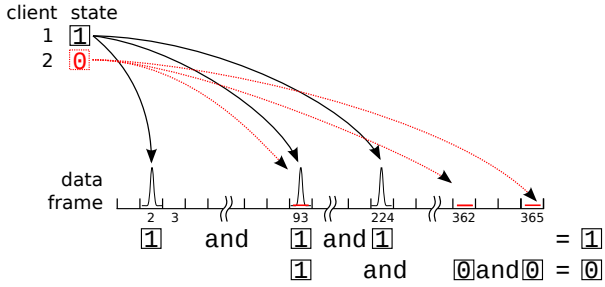
Colisión $\Rightarrow$ Error

CDMA + Filtro de Bloom (K=3)



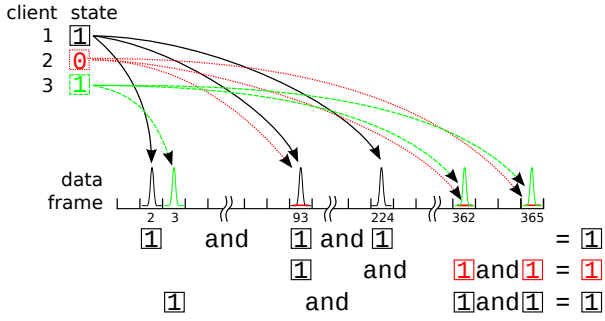
Inserta el bit '1' en la trama

CDMA + Bloom filter (K=3)



Inserta el bit '0' en la trama

CDMA + Bloom filter (K=3)

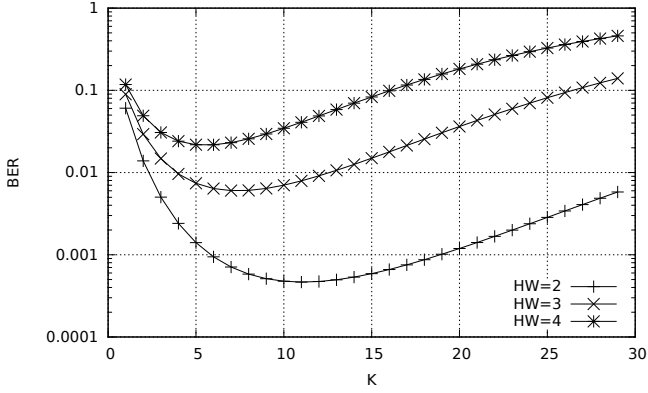


Inserta el bit '1' en la trama $\Rightarrow$ Error

K óptimo

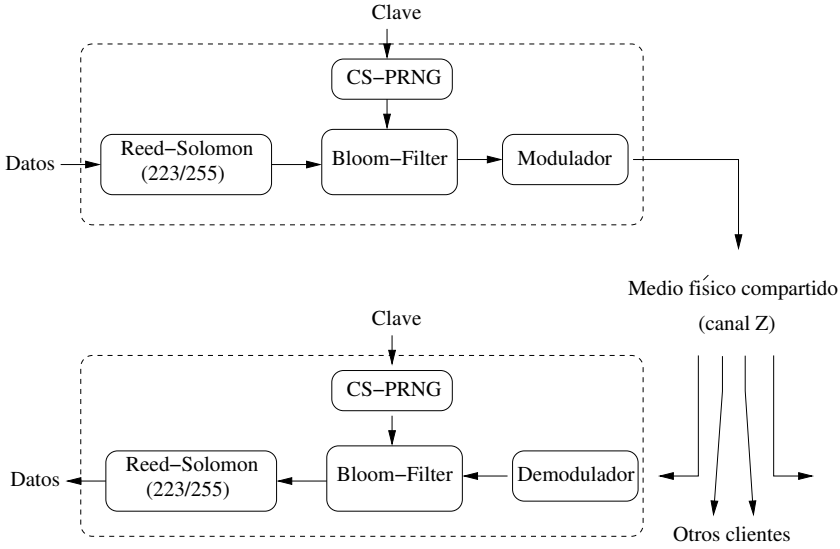
$$\text{BER} \approx \left(1 - \left(1 - \frac{1}{M}\right)^{N \cdot K \cdot m_1}\right)^K$$

- M es el tamaño de trama.
- N es la cantidad de usuarios.
- K es el parametró de repetición del filtro de Bloom.
- m_1 es la cantidad promedio de unos por símbolo.



Estimación del BER en función de K para $M = 4096$, m_1 varía de 2 a 4 y $N = 128$.

Diagrama esquemático



Minimización del peso de Hamming

- Peso de Hamming: cantidad de '1's en un dígito binario.
- Ej.:

$$HW(00101010) = 3$$

$$HW(00100000) = 1$$

- La minimización del HW es una representación o codificación numérica alternativa.

Minimización del peso de Hamming

- Peso de Hamming: cantidad de '1's en un dígito binario.
- Ej.:

$$HW(00101010) = 3$$

$$HW(00100000) = 1$$

- La minimización del HW es una representación o codificación numérica alternativa.
- En un canal Z, los '1' producen interferencia, los '0', no.

Minimización del peso de Hamming

Símbolo de 8-bits, Peso de Hamming=2, expansión a 24 bits

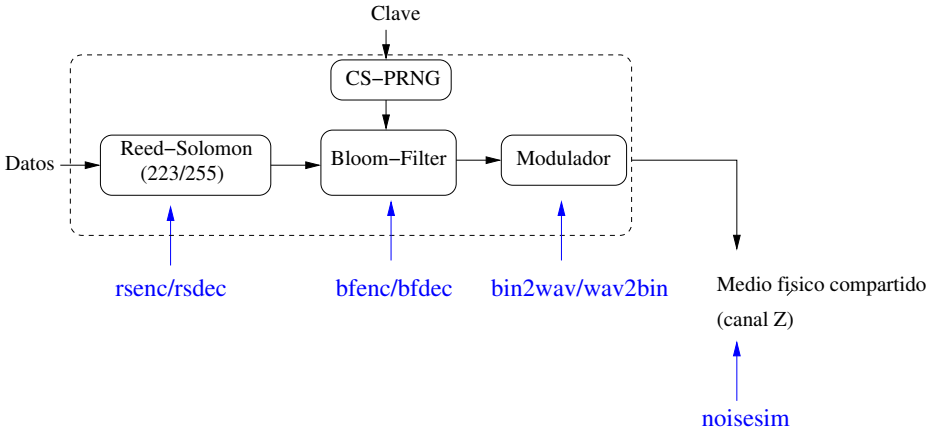
Dato	Entrada, HW=variable	Expansión HW=2
0	00000000	000000000000000011
1	00000001	000000000000000110
2	00000010	000000000000000101
3	00000011	000000000000001100
4	00000100	000000000000001010
253	11111101	100100000000000000
254	11111110	101000000000000000
255	11111111	110000000000000000

El peso de Hamming fijo previene ataques estadísticos en los datos codificados.

Simulaciones: software de prueba

- Framework de pruebas: Se implementó un módulo independiente por cada etapa.
- Utilizado C, C++ y Boost para mejor desempeño.
- Incluye un simulador de ruido óptico.
- Modulador/demodulador de audio.
- Modelo cliente/servidor para simulaciones distribuidas.

Simulación: software de prueba



Correspondencia de etapa con módulos de simulación

Simulación: software de prueba

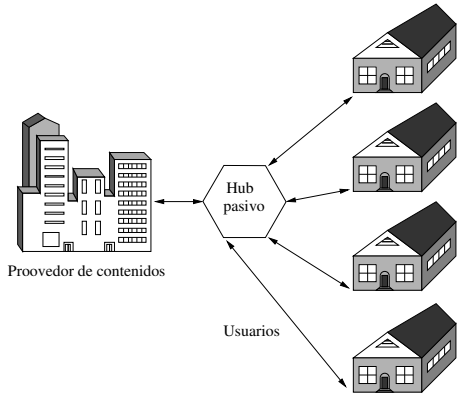
Ejemplo de linea de comando para lanzar la simulación:

```
./rsenc <testfile.in | ./scrambler ${SCRAMBLEBLOCK} >rs.out
./bfenc ${CLIENTES} < rs.out | ./noisesim -c ${CLIENTES} -r 16.6 >bfenc.out
./bfdec ${CLIENTES} <bfenc.out >bf.out
./descramble ${SCRAMBLEBLOCK} <bf.out | ./rsdec >rsdec.out
```

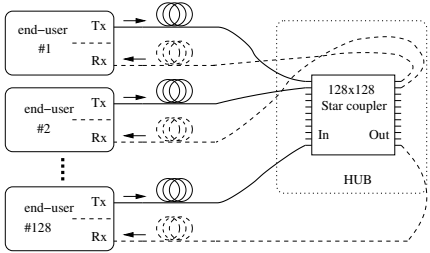
El BER (*bit error rate*) se calcula con la diferencia entre **testfile.in** y **rsdec.out**.

Implementación sobre red óptica

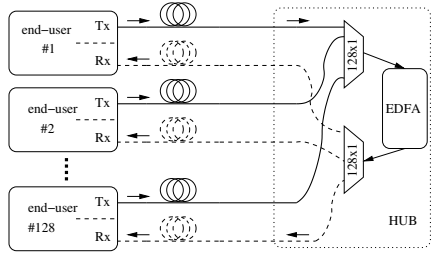
- Capaz de operar a 5 Gbps+
- Distancias hasta 10 km del nodo central (sin amplificación).
- Hasta 128 usuarios simultaneos.
- Diseño digital *custom* sobre FPGA.
- Utiliza transceptores ópticos SFP+ estandard



Implementación: Fibra óptica



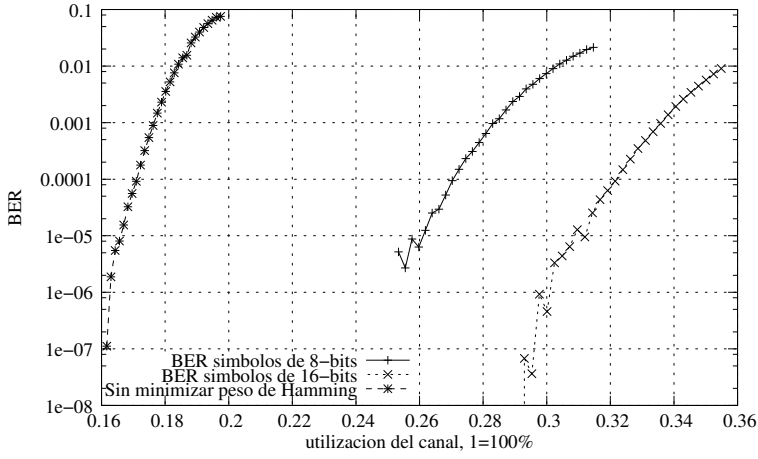
(a) Distribución via acoplador tipo estrella 1



(b) Distribución via EDFA

Diseño de red propuesto para la capa óptica

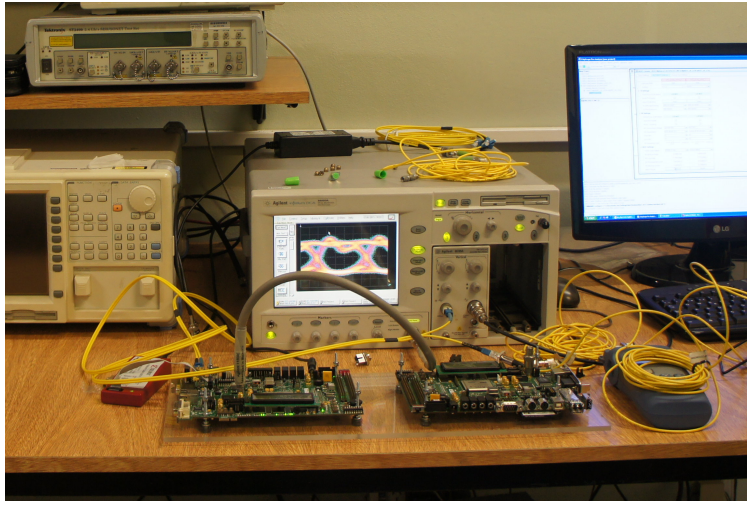
Implementación: Fibra óptica, Resultados (Simulaciones)



Desempeño 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.

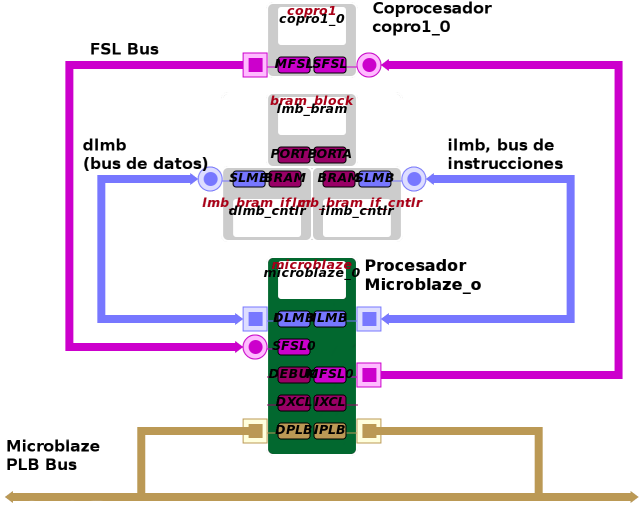
Implementación: Fibra Óptica

Placas de desarrollo Xilinx ML507

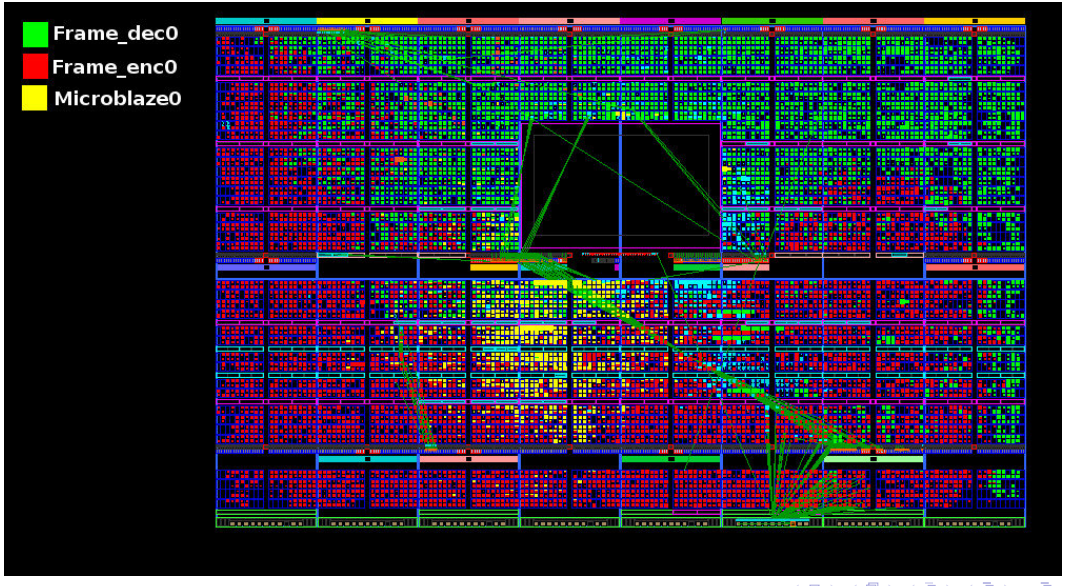


Implementación: Fibra óptica, FPGA

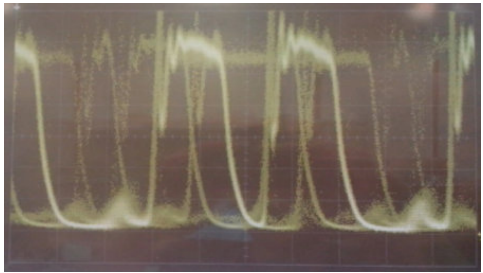
- CPU Microblaze (Debugging), 75 Mhz, sin DRAM
- Coprocesador, 100 Mhz
- Utilización (*Slices*): 9446 de 11200, 84 %
- Tiempo de sintetizado: aprox. 40 minutos (Core i7 2da generación)



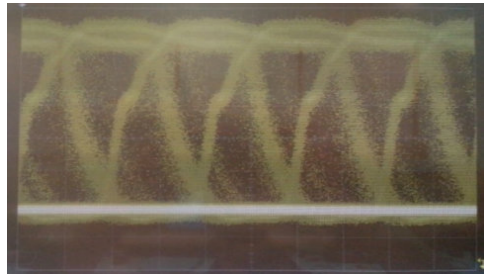
Implementación: Fibra óptica, FPGA



Implementación: Efectos de señal desbalanceada



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

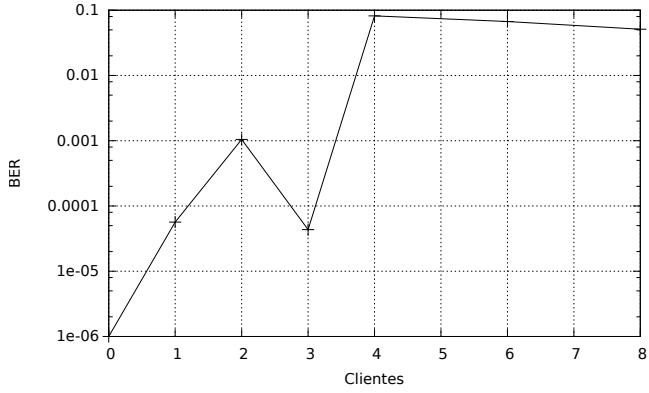


(d) Señal con 48 bits en uno por trama, 1100 ps por bit

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

Mediciones ópticas

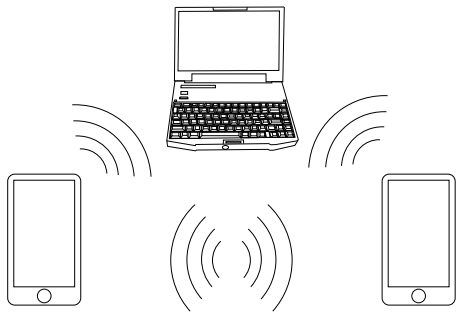
- Atenuador fijo en 10.85 DB
- Velocidad de enlace: 2.5 gbps
- SFP de link: sumitomo-electric-scp681 (S-16.1DDM)
- SFP de ruido: sumitomo-electric-scp681 (L-16.1)



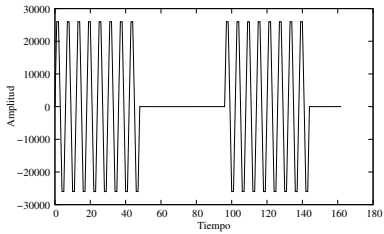
BER antes de corrección de errores

Implementación sobre red acústica

- Modem: 1 Khz de ancho de banda, 1 Kbps, portadora a 12 Khz y 16 Khz (inaudible).
- Distancias hasta 2 m del nodo central.
- Máximo de 8 usuarios.
- Implementación puramente en software.
- Utiliza hardware existente en celulares y notebooks (micrófonos y parlantes).



Medio acústico: modulación



Modulación OOK.

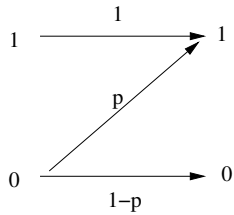
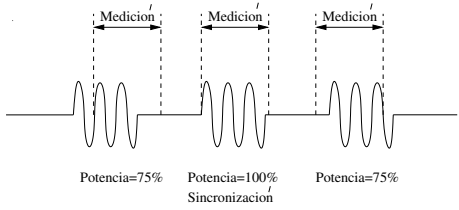


Diagrama de probabilidad: canal Z.

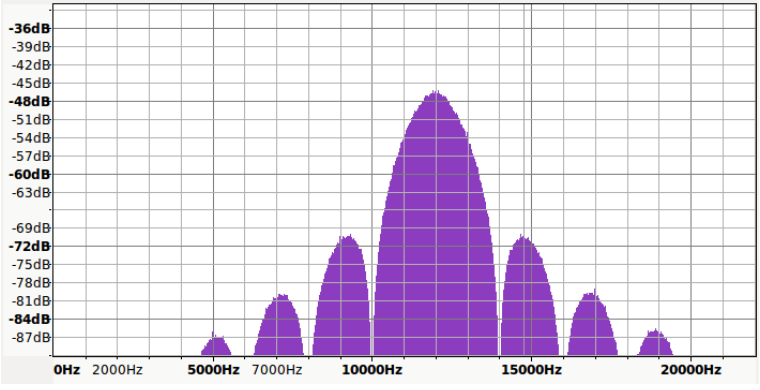
- Interferencia de OOK se aproxima a la de un canal Z.
- Baja densidad espectral (0.2 bits/s/Hz)

Medio acústico: sincronización



Sincronización de bit/nivel de decisión

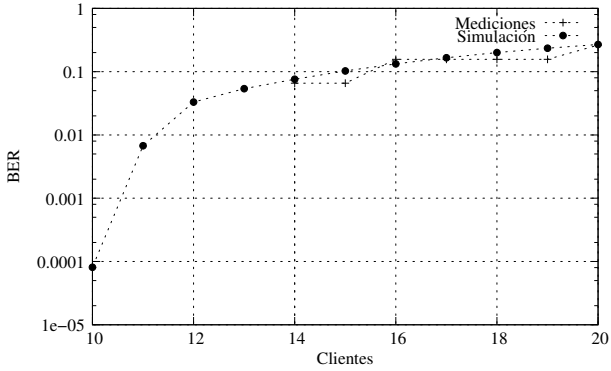
Medio acústico: características y espectro



Espectro de señal modulada, salida directa del modem.

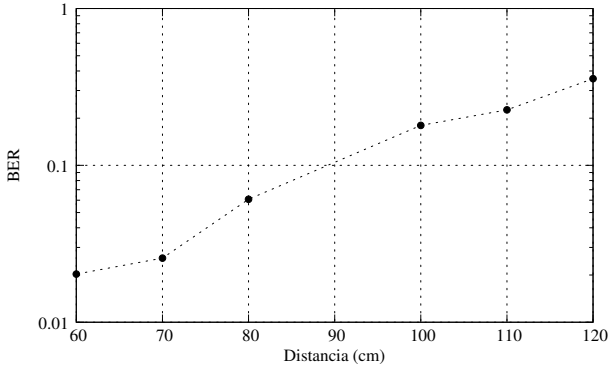
- Portadora a 12 Khz, modem funcionando a 1 Kbps en total
- Velocidades de 350 bps (2 usuarios) a 70 bps (10 usuarios)
- Dispositivos móviles: buen desempeño parlante/micrófono de 100 a 15 Khz

Medio acústico: resultados (simulaciones y mediciones)



BER *vs.* número de clientes

Medio acústico: resultados (mediciones)



BER *vs.* distancia

Conclusiones:

- Se propuso una arquitectura de red privada tipo time-hopping CDMA:

Conclusiones:

- Se propuso una arquitectura de red privada tipo time-hopping CDMA:
  - Para redes de difusión del tipo canal z.

Conclusiones:

- Se propuso una arquitectura de red privada tipo time-hopping CDMA:
  - Para redes de difusión del tipo canal z.
  - Utilizando filtros de Bloom y minimización de peso de Hamming.

Conclusiones:

- Se propuso una arquitectura de red privada tipo time-hopping CDMA:
  - Para redes de difusión del tipo canal z.
  - Utilizando filtros de Bloom y minimización de peso de Hamming.
  - Punto-a-Punto, y Punto-a-Multipunto.

Conclusiones:

- Se propuso una arquitectura de red privada tipo time-hopping CDMA:
  - Para redes de difusión del tipo canal z.
  - Utilizando filtros de Bloom y minimización de peso de Hamming.
  - Punto-a-Punto, y Punto-a-Multipunto.
  - **29 % de utilización del canal.**

Trabajos futuros:

- Sincronización segura.
- Encriptación autenticada.
- Autenticación de nodos y distribución de claves (*Forward Secrecy*).
- Implementación en otros medios. Ej. Radio.

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)*

Fin de la presentación

Muchas gracias por su asistencia.

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.

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.

Jay, John A., An overview of macrobending and microbending of optical fibers.
White Paper WP1212, Corning, 2010.