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

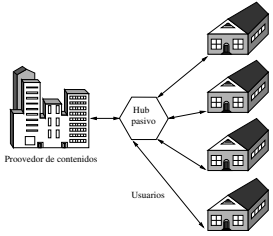
Alfredo Adrián Ortega
Instituto Tecnológico de Buenos Aires (ITBA)
aortega@alu.itba.edu.ar

30 de noviembre de 2015

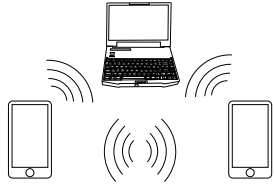
Contenido

Introducción

- Tema: Privacidad en redes de acceso utilizando CDMA.
- Algoritmo criptográficamente seguros.
- Medio de difusión (*broadcast*).
- Dos implementaciónes: comunicaciones ópticas y acústicas.



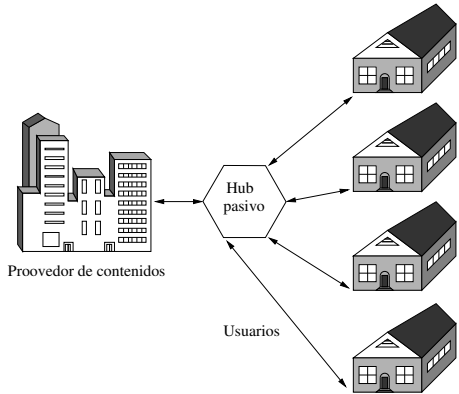
(a) Red óptica



(b) Red acústica

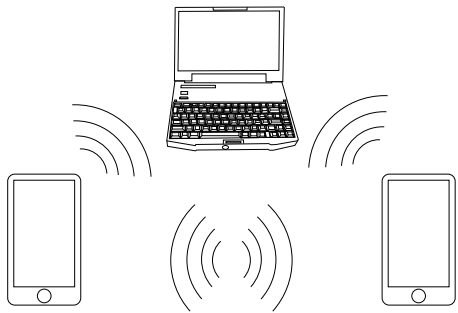
Implementación sobre red óptica

- 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



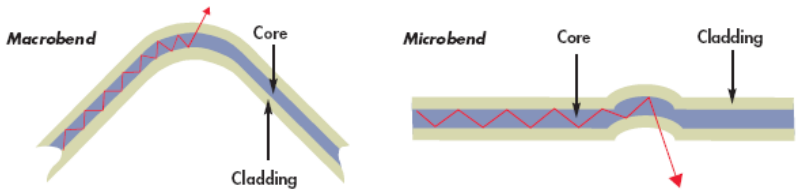
Implementación sobre red acústica

- 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).



Problemas a resolver

- 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]

Problemas a resolver (red óptica)

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.

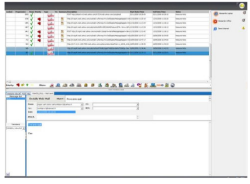
Intelligent Optical System 500 Data Sheet

Problemas a resolver (red óptica)

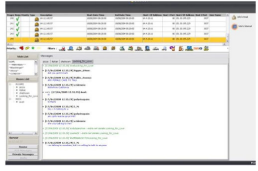
Monitor Internet, Webmail, VoIP, Internet, Mobile

Facebook

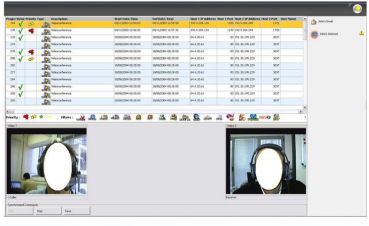
Webmail



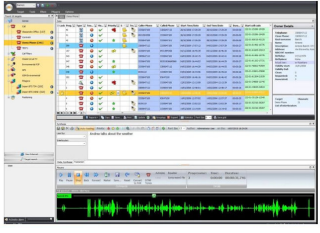
Chat



Internet Sessions: NetMeeting

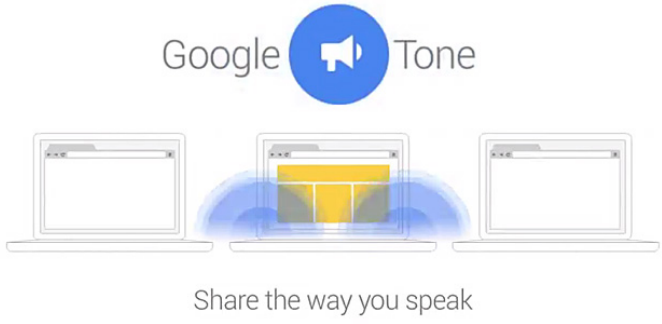


Wired / Wireless Phone Calls



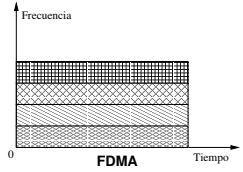
Problemas a resolver (red acústica)

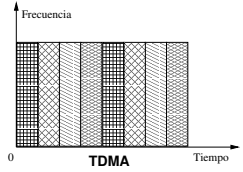
- Transmisión segura de claves/contacto/sistemas de TFA.
- Transacciones comerciales a corta distancia.
- Reemplazo de NFC, sin hardware específico.
- Ej. Google tone: *"An experimental chrome extension for instant sharing over audio"*

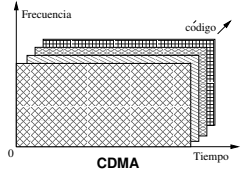


Solución propuesta

1. Utilizar `time hopping` para la separación en canales.
2. Utilizar algoritmos criptográficamente seguros para seleccion de canal.
3. Ante colisiones, utilizar algoritmos de corrección de errores específicos para canal Z.

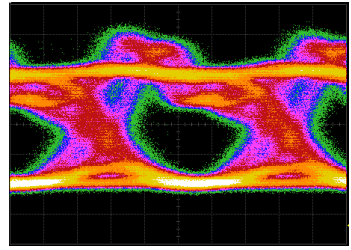






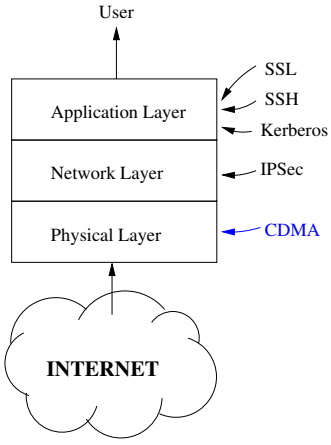
Desafíos

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. Bajo costo - utilización de hardware pre-existente.
5. En implementación acústica: bajo consumo de potencia y alta frecuencia de portadora.



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

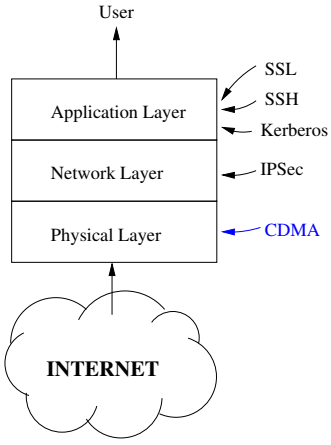
Seguridad en las capas de red



Modelo de red OSI simplificado

- SSH - solo punto-a-punto.
- SSL - protocolo muy complejo, muchas vulnerabilidades.
- Kerberos - idem SSL.

Seguridad en las capas de red



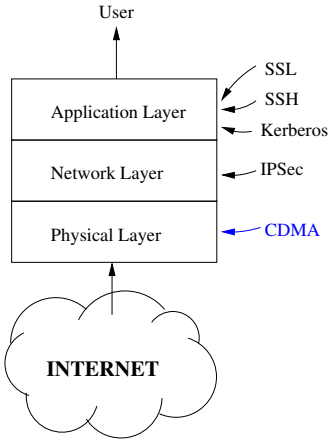
Modelo de red OSI simplificado

- SSH - solo punto-a-punto.
- SSL - protocolo muy complejo, muchas vulnerabilidades.
- Kerberos - idem SSL.

Desventajas:

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

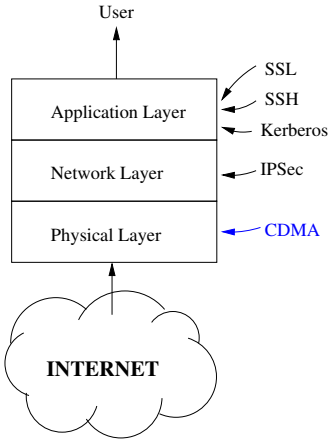
Seguridad en las capas de red



Modelo de red OSI simplificado

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

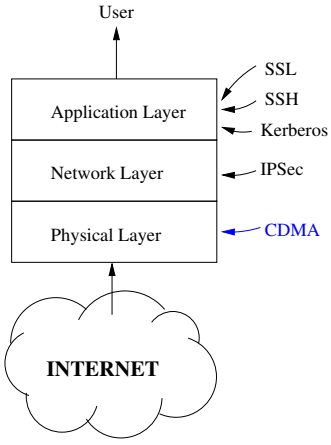
Seguridad en las capas de red



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:

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

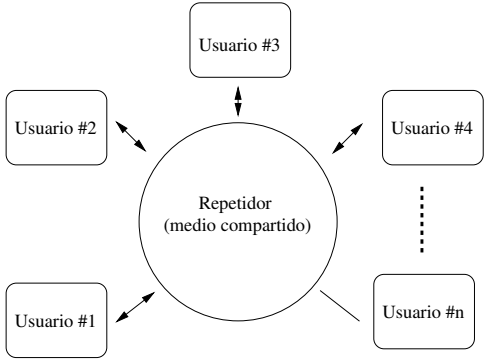
Filtro de Bloom: Provee corrección de errores asimétrica (en un canal Z)

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

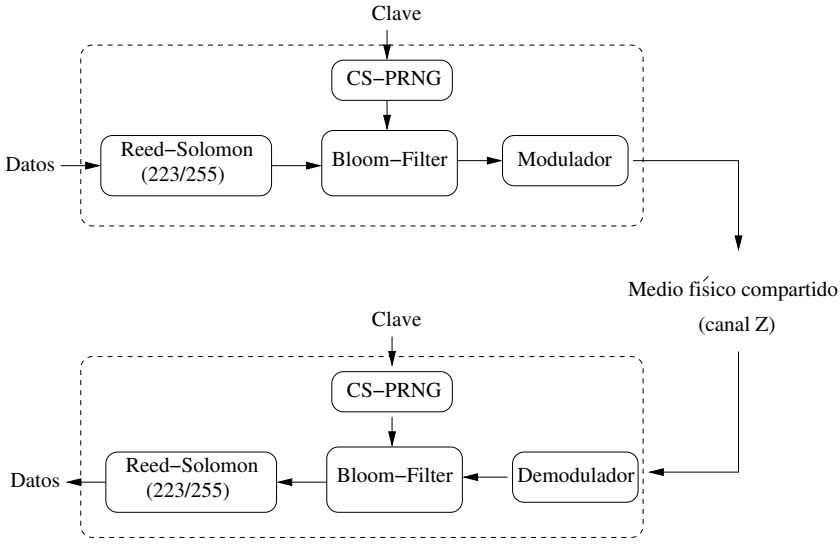
Ventajas:

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

Sistema propuesto: diseño de alto nivel



Sistema propuesto: diagrama esquemático



Canal Z

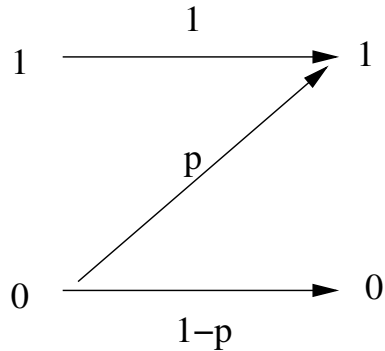
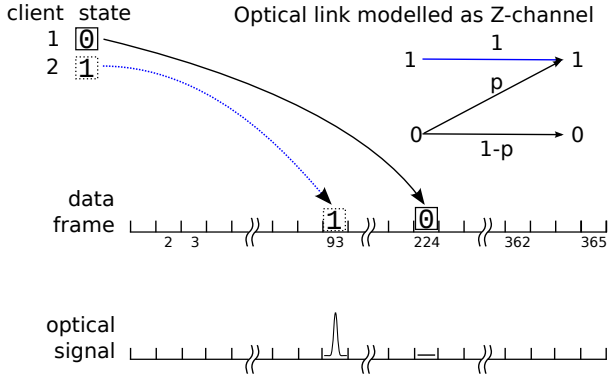


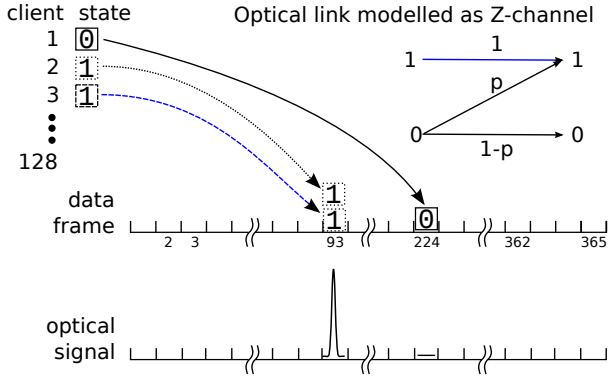
Diagrama de probabilidad del canal binario asimétrico o canal Z, donde p es la probabilidad de error.

Selección de casillero aleatoria: *time hopping*



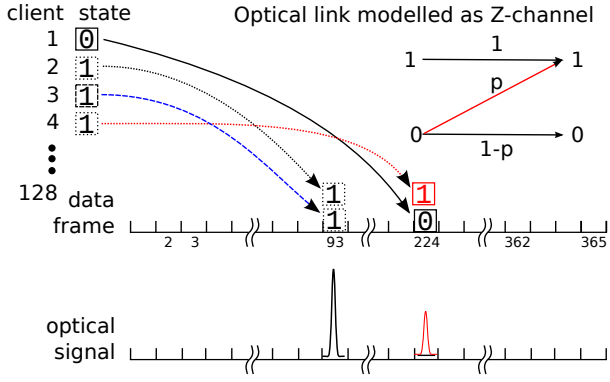
No hay colisión

Selección de casillero aleatoria: *time hopping*



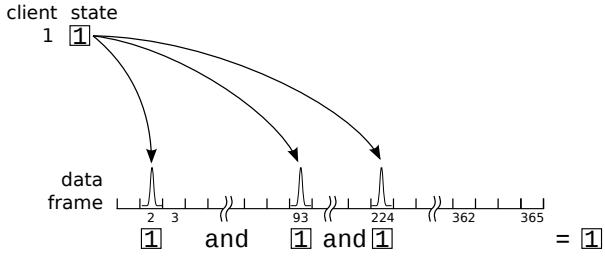
Colisión $\Rightarrow$ Resultado OK

Selección de casillero aleatoria: *time hopping*



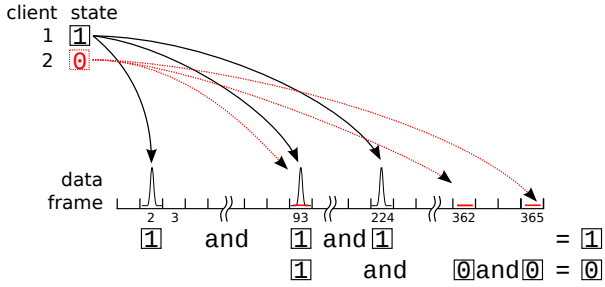
Colisión $\Rightarrow$ Error

CDMA + Filtro de Bloom (K=3)



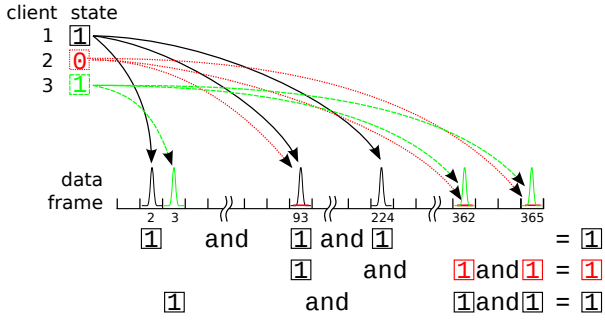
Inserta el bit '1' en la trama

CDMA + Bloom filter (K=3)



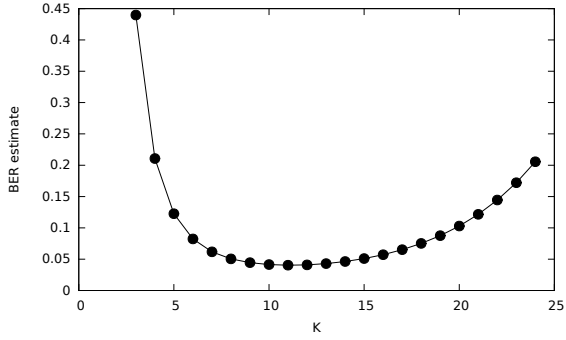
Inserta el bit '0' en la trama

CDMA + Bloom filter (K=3)



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

K óptimo



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 del peso de Hamming: origen

Origen de la técnica

- Peso de Hamming: cantidad de '1's en un dígito binario.
- En un canal Z, los '1' producen interferencia, los '0', no.
- Ej.:

$$HW(00101010) = 3$$

$$HW(00100000) = 1$$

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

Minimización del peso de Hamming: origen

Sistemas de numeración

- Mas extendido: números arábigos.
- Originalmente de India, documentado e introducido a Europa por Al-Jwarizmi.

Dada un conjunto de n dígitos ordenados d,
con posición p y base B, el valor numérico V es:

$$V = \sum_{n=0}^{n-1} B^p * d$$

Ej.

$$1685 = 10^3 * 1 + 10^2 * 6 + 10^1 * 8 + 10^0 * 9$$

Minimización del peso de Hamming: origen

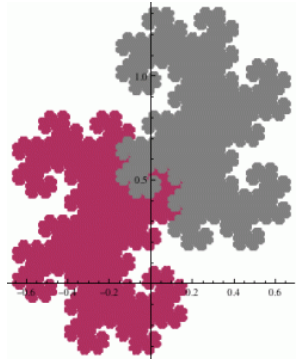
Sistemas de numeración: Ejemplos

- Bases no estandard, Ej.: Negabinario, base -2.

$$V = \sum_{n=0}^{n-1} (-2)^p * d$$

- Sistema numeral *Quater-imaginario*, base $-2i$, por [Knuth, Donald E].

$$V = \sum_{n=0}^{n-1} (2i)^p * d$$



Dragón de Davis-Knuth : fractal asociado a la base $(-1 \pm i)$

Minimización del peso de Hamming: origen

Sistemas de numeración: Ejemplos

- Códigos no regulares: Código Gray
- Dígitos con signo. Ej.:

$$1685 = 1000 * 1 + 100 * 6 + 80 * 10 + 5$$

pero también:

$$1685 = 169(-5) = 1000*1+100*6+90*10+(-5)$$

y también:

$$1685 = 169\bar{5} = 17\bar{1}\bar{5}$$

- Usado en el lenguaje Punjabi.

DECIMAL	BINARIO	GRAY
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Código Gray

Minimización del peso de Hamming: origen

Sistemas de numeración: Dígitos signados

- Existe más de una representación posible por número.
- La representación canónica de dígitos signados (CSD) es util:
  La probabilidad digitos no-cero es $\frac{1}{3}$.
  Usando dígitos binarios es $\frac{1}{2}$.
- Primeramente el sistema propuesto utilizó esta representación.
- Luego se utilizó una tabla con símbolos optimizados con un peso de Hamming fijo.

Binario:	001010111
CSD:	$010\bar{1}0\bar{1}00\bar{1}$

Minimización del peso de Hamming

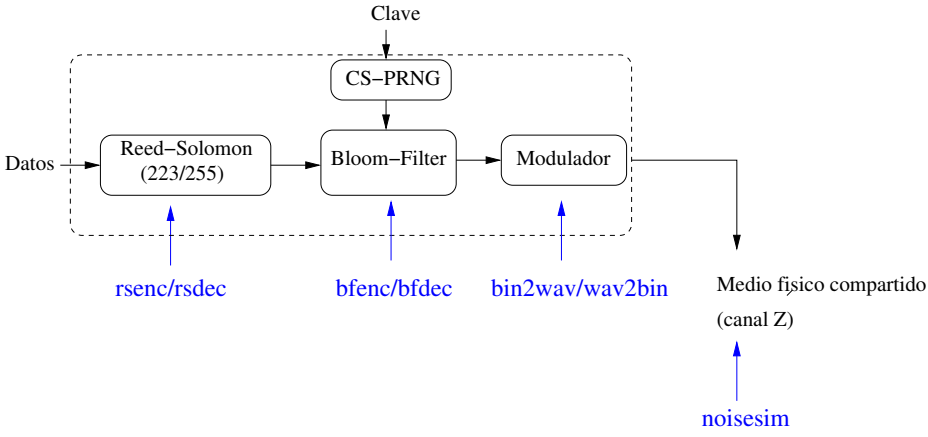
Símbolo de 3-bits, Peso de Hamming=2, expansión a 5 bits

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

Simulación: 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

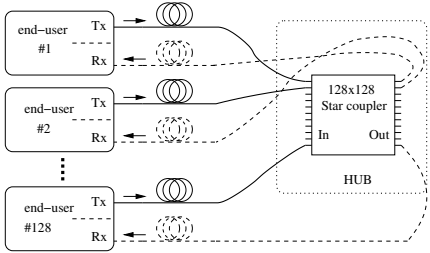
Simulación: software de prueba

Ejemplo de linea de comando para lanzar la simulación:

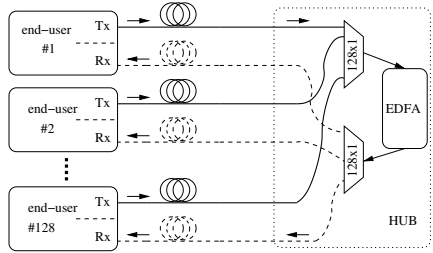
```
./rsenc <testfile.in | ./scrambler ${SCRAMBLEBLOCK} >rs.out
./bfenc ${CLIENTES} < rs.out | ./noisesim -c ${CLIENTES} -r 16.6 >bfenc.out
./bfdec ${CLIENTES} <bfenc.out >bf.out
./descramble ${SCRAMBLEBLOCK} <bf.out | ./rsdec >rsdec.out
```

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

Implementación: Fibra óptica



(c) Distribución via acoplador tipo estrella 1

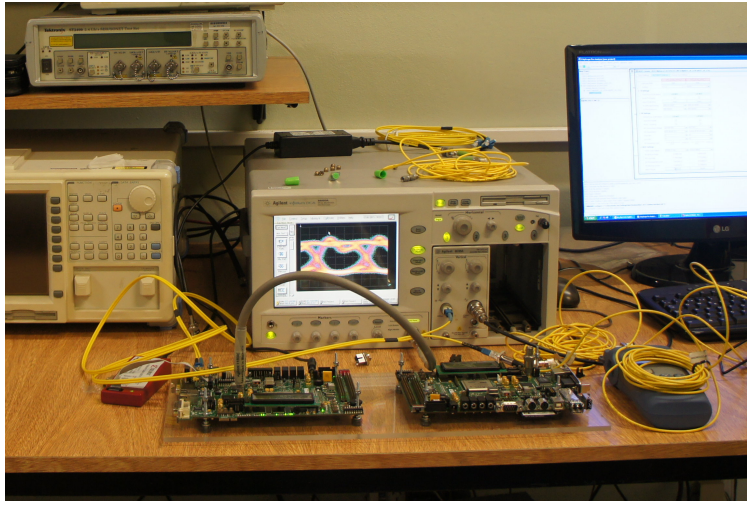


(d) Distribución via EDFA

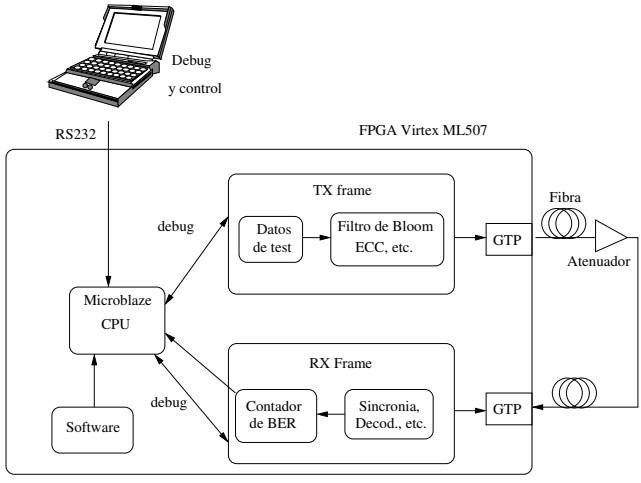
Diseño de red propuesto para la capa óptica

Implementación: Fibra Óptica

Placas de desarrollo Xilinx ML507

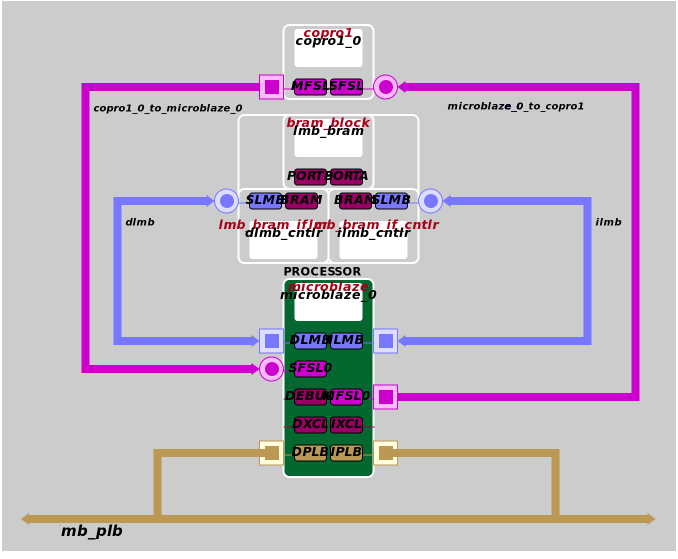


Implementación: Fibra óptica

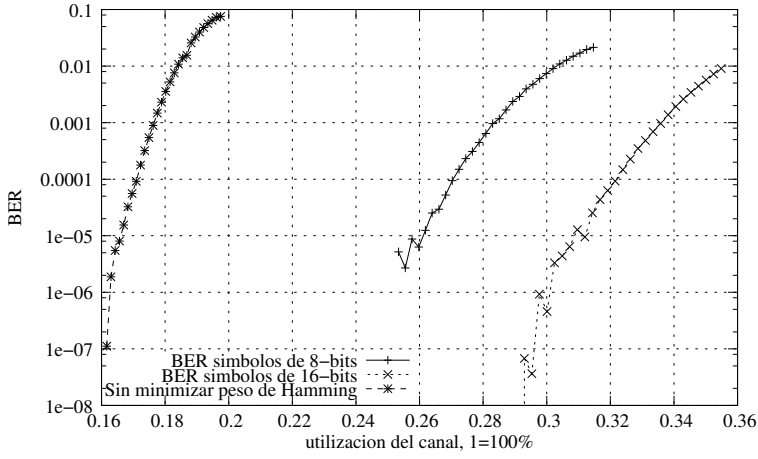


Diseño lógico de alto nivel sobre FPGA

Implementación: Fibra óptica, FPGA

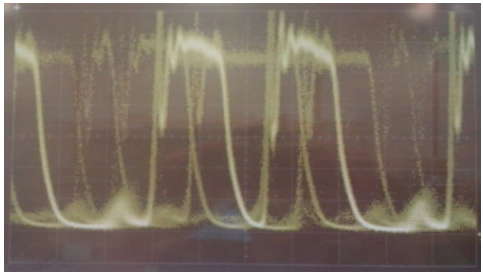


Implementación: Fibra óptica, Resultados (Simulaciones)

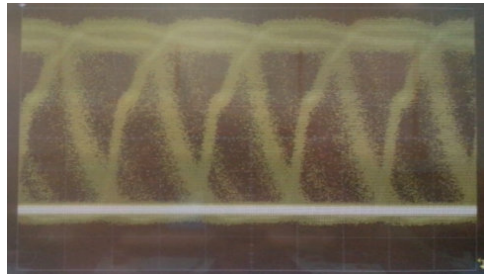


Desempeño del sistema con respecto a la expansión de símbolo. Simulación numérica de un enlace de 10 Gbps con 128 clientes, M=4096 y K=9.

Implementación: Efectos de señal desbalanceada



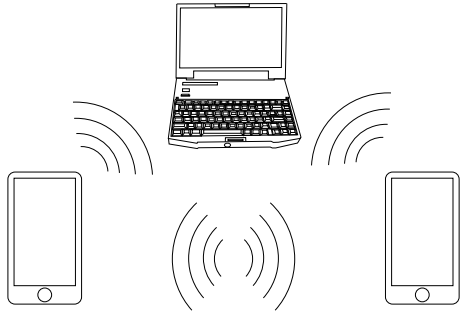
(e) Señal con 256 bits en uno por trama (8B/10B), 400 ps por bit



(f) 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.

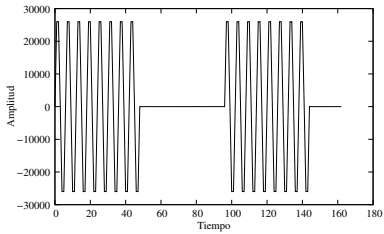
Medio acústico: introducción



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



Modulación OOK.

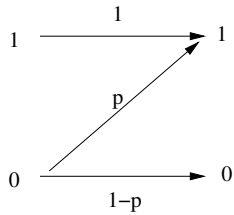
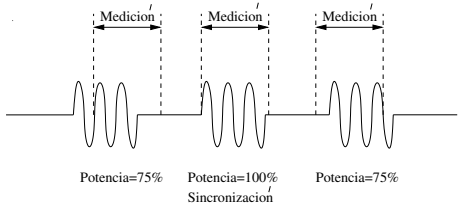


Diagrama de probabilidad: canal Z.

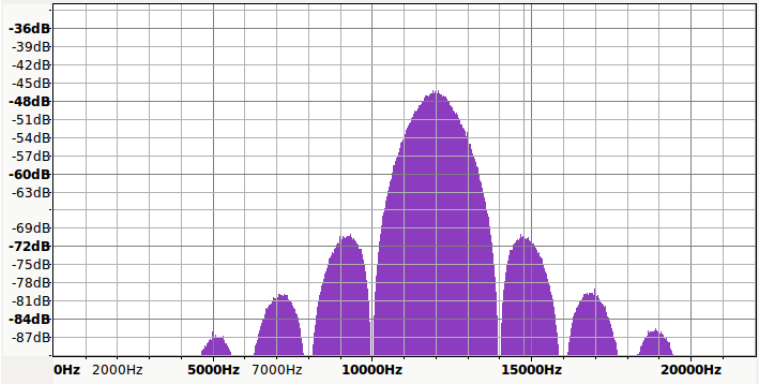
- Interferencia de OOK se aproxima a la de un canal Z.
- Baja densidad espectral (0.2 bits/s/Hz)

Medio acústico: sincronización



Sincronización de bit/nivel de decisión

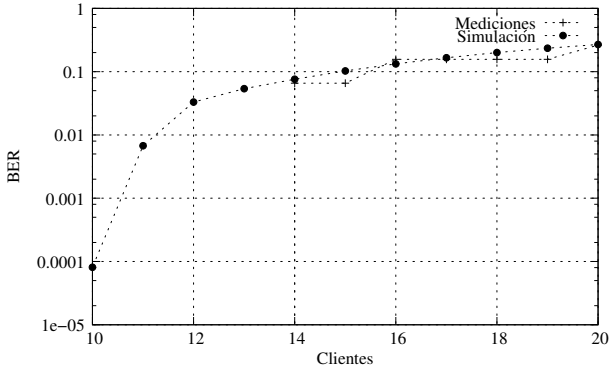
Medio acústico: características y espectro



Espectro de señal modulada, salida directa del modem.

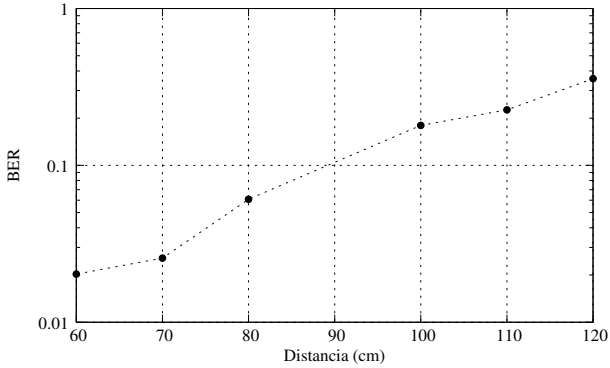
- Portadora a 12 Khz, modem funcionando a 1 Kbps en total
- Velocidades de 350 bps (2 usuarios) a 70 bps (10 usuarios)
- Dispositivos móviles: buen desempeño parlante/micrófono de 100 a 15 Khz

Medio acústico: resultados (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)*

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.


Knuth, Donald E.
An Imaginary Number System.
1960


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