Ultrafast Optical Processing & Information Security

Paul Prucnal
February 23, 2011

Wednesday July 27th, 3:30pm - 4:00pm
Double Tree Hotel, 4355 US Route 1, Princeton, NJ
Information security has many challenges....
Information security has many challenges....

...some of which have been addressed using ultrafast optical signal processing.
Total internal reflection governed by Snell’s Law with $\Delta n \sim 1\%$
Group Velocity Dispersion

Different spectral components of light travel at different velocities spreading the pulse.

Dispersion limits the maximum bit rate due to inter-symbol interference.
Evolution of Fiber Optic Transmission Capacity

(normalized for a 1,000 km transmission distance)

Dispersion limits maximum bit rate due to inter-symbol interference

D J Richardson Science 2010;330:327-328
Devices for Dispersion Compensation

“Standard” single mode fiber

“Dispersion compensating fiber”

Compact “Fiber Bragg Grating”

Refractive index gratings made by exposure to uv light
Physical Layer Security using Optical Signal Processing

Hiding optical signals in plain sight

Existence of Transmission
Steganography: Hiding Signals in Plain Sight

The *existence* of a message may itself be sensitive information.

The origins of steganography are rooted in ancient Greece:

- Messages were carved in wood and hidden by covering with wax.
- Herodotus tells of tattooing a message on a slave's shaved head, which was then hidden covered by hair regrowth. Not ultrafast processing!

Spread spectrum is used in wireless military communications to hide signals below noise.

Rock concert pass written in invisible (UV-sensitive) ink
Temporal Hiding

In optically dispersive media:
- Pulse spreading reduces its amplitude.
- The power at each frequency and the spectrum remain unchanged.
- Negative dispersion restores the pulse to its original shape.
Temporal Hiding

In optically dispersive media:
- Pulse spreading reduces its amplitude.
- The power at each frequency and the spectrum remain unchanged.
- Negative dispersion restores the pulse to its original shape.

Dispersive media:
- Single mode optical fiber
- Fiber Bragg gratings
Temporal Hiding using Chirped Fiber Bragg Gratings

Private Channel Alone

Before Spreading  |  After Spreading  |  After Compression

Public channel without and with the stealth signal
Physical Layer Security using Optical Signal Processing

Security by Obscurity

Interception
Hiding via Frequency Hopping

Frequency-hopping optical CDMA network
- Private and public channels overlap both temporally & spectrally.
- Use in conjunction with dispersive spreading
- To detect the private channel, need both the correct decoder and dispersion compensation.

Fiber Bragg Grating Encoder

Decoder and Optical Thresholding

Picosecond laser pulse

One data bit
Multiaccess Interference Rejection for Scaling OCDMA

2.5 Gbit/sec
Carrier-hopping prime codes (4,17)
\( K = 4 \log_2 17 = 16.3 \)

Codes 1 + 2 “obscure” each other

User 1

User 2

OCDMA Encoders

OCDMA Decoder 1

Optical Thresholder

Code 1 recovered
Eavesdropping on Optical CDMA

Eve’s difficulty in guessing Alice’s code sequence increases with code cardinality. The amount of information Eve requires to have the same detection performance as Alice is called the “effective key length.”

\[ K_{OOK}^{\text{eff}} = w \log_2 N_T \]

- \( w \) = # wavelengths
- \( N_T \) = number of chips

Requires very large code sets to be effective.
Physical Layer Security using Optical Signal Processing
All-optical encryption eliminates the electromagnetic signature and enables encryption at any line rate.
All-optical data encryption eliminates the electromagnetic signature and enables encryption at any line rate.
“Self phase modulation” for pulses of high intensity in optical fiber

\[ i \frac{\partial A}{\partial z} + \gamma |A|^2 A = 0 \]

for \( A = A_0 e^{i \Delta \phi} \),

\[ \Delta \phi(z) = \gamma |A_0|^2 z \]

Pulses experience an intensity-dependent phase shift.
Optical nonlinearity limits maximum bit rate due to inter-channel crosstalk.

(normalized for a 1,000 km transmission distance)
Nonlinear Fiber-Based Optical Encryption

Nonlinear Fiber based XOR Gate

Data When Key is all zero

Key When Data is all zero

XOR Output

Encoded Data Out with code swapping
Physical Layer Security using Optical Signal Processing

Communicating through jamming
Iraq Ground Scanner – IED Jammer
UNCLASSIFIED
Interference Canceller System Diagram

Approx 1 meter

Jamming Cancellation Box
Mach Zehnder Electro-Optic Modulator

Modulation is proportional to the received interference.

Modulation is inversely proportional to the transmitted jamming signal.
Mach Zehnder Electro-Optic Modulator

Modulation is proportional to the received interference

Modulation is inversely proportional to the transmitted jamming signal

Optical Intensity

Voltage

$V_{bias} - 2V_\pi$

$V_{bias} - V_\pi$

$V_{bias}$

$V_{bias} + V_\pi$

$V_{bias} + 2V_\pi$
Mach Zehnder Electro-Optic Modulator

Modulation is proportional to the received interference

Modulation is inversely proportional to the transmitted jamming signal
Mach Zehnder Electro-Optic Modulator

Modulation is proportional to the received interference

Modulation is inversely proportional to the transmitted jamming signal
Narrowband and Broadband Cancellation

Narrowband Measurement

~80 dB cancellation

Broadband Measurement

Min: ~45 dB cancellation
Max: ~70 dB cancellation
<table>
<thead>
<tr>
<th>Function</th>
<th>Approach</th>
<th>Optical Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide optical signals</td>
<td>Temporal spreading</td>
<td>FBG</td>
</tr>
<tr>
<td></td>
<td>Spectral spreading</td>
<td>ps laser</td>
</tr>
<tr>
<td>Reduce intercept probability</td>
<td>Optical CDMA</td>
<td>FBG + all-optical thresher</td>
</tr>
<tr>
<td>Ultrafast data encryption</td>
<td>AND logic</td>
<td>Solution interactions</td>
</tr>
<tr>
<td></td>
<td>XOR</td>
<td>2-input nonlinear fiber switch</td>
</tr>
<tr>
<td>Broadband jamming cancellation</td>
<td>Translate RF signal to optical domain</td>
<td>Electrooptic counter-phase modulators</td>
</tr>
<tr>
<td>Identification, decisions, learning</td>
<td>Hybrid spike processing</td>
<td>SOA integrator + FIR + thresher</td>
</tr>
</tbody>
</table>