Cycle 5:
Physical Layer and Wireless

CS 436: Spring 2018
Matthew Caesar
Physical Media
Today: Physical Media

• Networks are made up of devices and communication links

• Devices and links can be physically threatened
  • Vandalism, lightning, fire, excessive pull force, corrosion, wildlife, weardown
  • Wiretapping, crosstalk, jamming

• We need to make networks mechanically resilient and trustworthy
AT&T Cables Vandalized, $250,000 Reward Offered for Information

Two of the company’s main fiber optic lines were cut in Del Mar Thursday morning, leading to a widespread communications outage.

By Tony Shin and Monica Garske | Friday Jun 15, 2012 | Updated 7:00 AM PST

North County experienced a widespread communications outage Thursday after an unidentified person or vandals deliberately cut two main fiber optic lines belonging to AT&T.

According to information released by the company, the lines were cut two miles apart, making it unlikely that the cause was the work of a single individual.

North County was largely unaffected, while the Los Angeles area was hit hard. The company said it was not sure how long it would take to resolve the issue.

Cable theft costs Telkom R863m

Cable theft between April last year and the end of January has cost Telkom R863-million, the telecommunications provider said on Monday. In a statement, Telkom said the “alarming surge” in cable theft was “the biggest inhibitor in its capability to improve service and deliver on its obligations to customers.”

Fiber Optic Cable System Vandalism A National Security Problem

On April 9th a criminal incident impacting nearly a million people in three counties of California was largely unnoticed by the media, both national and local. This incident has far reaching implications far beyond the scale and scope of the San Jose incident.

The San Jose incident, as reported by SFGate, was probably not a random act of vandalism, but a targeted attack on the telecommunications network infrastructure. The attackers were able to cut off access to the internet for millions of people in what appeared to be a coordinated attack.

$50,000 REWARD

Verizon takes great pride in the reliability of its service and quickly makes necessary repairs. Federal and State laws carry stiff penalties (imprisonment and fines) for the intentional destruction of telecommunications facilities or assaults against Verizon workers.

Verizon is offering a reward of up to $50,000 to the first person who provides information leading to the arrest and prosecution of any person who intentionally:

- Damages Verizon cables or facilities
- Causes or attempts to cause physical injury to individuals
This lecture

• Methods for physical communication

• Overview of copper, optical, and wireless communication technologies

• Wire mechanics, attacks, and countermeasures
How can two computers communicate?

• Encode information into physical “signals”
• Transmit those signals over a transmission medium
Types of Media

• Metal (e.g., copper)

• Light (e.g., optical fiber)

• EM/RF (e.g., wireless 802.11)
Wireless Networks
Current can flow through wires

Direction of flow of electrons

Direction of flow of electric current

Cell
Current flow in wires induces magnetic field
Magnetic field induces current flow

- This can be bad (crosstalk)
- This can be good (can transmit data)
We can use EM leakage to transmit data

- Electronic oscillator generates alternating current at a frequency (carrier signal)
  - Rate of oscillation: Wavelength of signal
  - Information is piggybacked by modulating carrier signal
- Bandpass filter used on receiver to extract information signal
Path Loss Effects

- Wireless signals are like light
  - Just a different wavelength along EM spectrum
- They interact with physical objects in similar ways
  - Can be bad – can degrade signal
  - Can be good – can leverage this to improve signal strength/range
Path Loss Effects
Wireless signals propagate like waves

- Propagate at speed of light in vacuum
  - Propagation speed independent of wavelength
- Matching wavelengths construct, opposing wavelengths destruct
Wireless Signals can self-interfere

• Could be a good thing, if they construct
• Could be a bad thing, if they destruct
Fresnel Zone

- Ellipsoid drawn between transmitter and receiver should be kept clear from obstacles
  - Heuristic: max obstruction <40%, recommended <20%
Fresnel Zone radius computation

\[ F_n = \sqrt{\frac{n \lambda d_1 d_2}{d_1 + d_2}}, \quad d_1, d_2 \gg n \lambda \]

- Online calculator:
  https://www.everythingrf.com/rf-calculators/fresnel-zone-calculator

- \( F_n \) is the \( n \)th Fresnel zone radius,
- \( d_1 \) is the distance of P from one end,
- \( d_2 \) is the distance of P from the other end,
- \( \lambda \) is the \textit{wavelength} of the transmitted signal.
How physical objects affect wireless signals

- Different materials affect reflection/absorption/refraction/etc in different ways
Atmospheric Opacity

- Gamma rays, X-rays and ultraviolet light blocked by the upper atmosphere (best observed from space).
- Visible light observable from Earth, with some atmospheric distortion.
- Most of the infrared spectrum absorbed by atmospheric gases (best observed from space).
- Radio waves observable from Earth.
- Long-wavelength radio waves blocked.
Is attenuation good or bad?
Example: Two APs

- What if not enough capacity?
Example: Nine APs

• Problem:
Example: Nine APs

- More attenuation better for dense deployments
Example: Nine APs

- More attenuation better for dense deployments
Atmospheric attenuation in wifi spectrum

- 802.11ad: 60 Ghz chosen because of increased atmospheric attenuation
Increased capacity with spectrum division

• 802.11 supports different “channels” / wavelengths
• Put nearby APs on different wavelengths
General Problem: Graph Coloring

- Vertices are APs, edges denote reachability
- Number of channels/colors needed a function of graph connectivity
How other physical objects affect wireless signals

- Attenuation in water to 1/3:
  - Pure water: 8.01Km
  - Drinking water: 44.54m
  - Sea water: 8.91mm

- Humans similar to sea water
  - More fat → more attenuation

- Trees: leaves and rain increase attenuation
“Polarization” of EM Waves

• Signals are “polarized” in direction of current flow
Polarization options

- Horizontal Polarized
- Vertical Polarized
- Dual Polarized
- Cross Polarized
- Right Hand Circular Polarized
- Left Hand Circular Polarized
Antenna placement for polarization

• You don’t know how your users are polarized → propagate signals for both
  • Some APs propagate two polarizations
  • Can manually configure antennas

• Also covers vertical and horizontal space
Antenna Types: Omnidirectional

- Radiates equally in all directions in one plane
  - Power decreases above/below plane
- Widely used in APs, NICs
Antenna Types: Directional (Yagi)

- Multiple parallel elements in a line
- Substantial increase in directionality and gain
Antenna Types: Directional (Parabolic)

- Reflector must be substantially larger than wavelength
- Metal screen reflects as well as solid dish if spaces $< \frac{1}{10}$ wavelength
How to choose an antenna

- **Directionality**: do you want to light up a particular area, or entire surrounding region?

- **Gain**: how much “reach” the antenna has compared to an omnidirectional antenna

- **Bandwidth**: range of frequencies over which the antenna operates effectively
How can wireless hosts share the spectrum?

• What happens when two hosts transmit at the same time?
  • Collision

• What should we do about collisions?
How to mitigate collisions

A few options:

1. Just let transmissions collide
   - Problem: data gets corrupted

2. Collision Detection (CD): Let transmissions collide, but detect collisions
   - If sender knows their packet collided, they can retransmit

3. Collision Avoidance (CA): Try to prevent collisions
Collision Detection (wired)

0:000 Packet transmission begins

0:016 Collision detected! Start ignoring packet

0:022 Collision detected! Packet transmission unsuccessful. Wait and retry.
0:008 Packet transmission begins

0:016 Collision detected! Start ignoring packet

Collision!
Collision Detection (wired, small packets)

0:000 Packet transmission begins

0:008 Packet transmission begins

0:016 Collision detected! Start ignoring packet

0:016 Collision detected! Start ignoring packet

0:022 Finished transmitting packet successfully! Start transmitting next packet.

0:008 Packet transmission begins

Collision!
Collision Detection, Wireless

-30dB (maximum practically-achievable signal strength)

-65dB (minimum signal strength for applications that require reliable, timely delivery)

-70dB (minimum signal strength for reliable delivery)

0:000 Packet transmission begins

0:008 Packet transmission begins
Collision Avoidance, Wireless

Can I have the channel please? My MAC address is XX:XX:XX:XX

Request To Send / RTS

Yes, XX:XX:XX:XX, you may transmit.

Clear To Send / CTS

I just saw an ACK— whoever was transmitting before is done, so I can send a RTS if I need to send packets.

Data Packet
Can I have the channel please? My MAC address is XX:XX:XX:XX

Request To Send / RTS
How to know where access points are?

- Access points periodically send beacon frames
  - Contain SSID, supported rates, transmission parameters
  - Default interval of 100ms
- NICs scan all channels searching for beacons
  - Can show list to user, eg sorted by signal strength or preference
  - NICs can also actively send probe requests to actively scan
AP Association Process

- Done on first connection
- If signal becomes low, client repeats process to be associated with another AP
AP Deployment

• Try to use the same SSID when possible, to enable automated roaming to the highest-quality AP
• APs that use the same channel should be installed as far away from each other as possible to minimize interference
• AP cell size should overlap by 15-25% to ensure that there are no gaps in coverage and to ensure a roaming client will always have a connection visible
Copper-based Networks
Connections and Cabling
Background: Electrical Current

- Usually free electrons hop around randomly
- However, outside forces can encourage them to flow in a particular direction
  - Magnetic field, charge differential
  - This is called current
  - We can vary properties of current to transmit information (via waves, like dominos, as electron drift velocities are very slow)
Conductors vs. Insulators

- **Conductor**: valence electrons wander around easily
  - Copper, Aluminum
  - Used to carry signal in cables
- **Insulator**: valence electrons tightly bound to nucleus
  - Glass, plastic, rubber
  - Separates conductors physically and electrically
- **Semiconductor**: conductivity between insulator and conductor
  - Can be easily made more conductive by adding impurities

<table>
<thead>
<tr>
<th>Material</th>
<th>Resistivity (ohm m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glass</td>
<td>$10^{12}$</td>
</tr>
<tr>
<td>Mica</td>
<td>$9 \times 10^{13}$</td>
</tr>
<tr>
<td>Quartz</td>
<td>$5 \times 10^{16}$</td>
</tr>
<tr>
<td>Copper</td>
<td>$5 \times 10^{-8}$</td>
</tr>
</tbody>
</table>
Common Conductors

- **Copper**: cheap, lower operating temperature, lower strength
- **Aluminum**: lightweight and cheap, but less conductive than copper
- **Silver**: most conductive material, but very high price
- **Nickel**: improved strength, higher resistance
- **Tin**: improved durability and strength, but higher resistance
Coating Copper to Improve Resilience

• Coating copper can provide additional properties
  • Done by “hot dipping” or electroplating

• Tinned copper: corrosion protection, easier to solder
  • Industrial ethernet deployments, environments exposed to water such as ships

• Silver plated copper: better conduction, operation over wider temperature range (-65°C to 200°C). Commonly used in aerospace applications

• Nickel-plated copper: corrosion protection, operation over wider temperature range (thick plating can withstand 750 deg C), reduced high-frequency loss
Reducing Resistance from the Skin Effect

• Alternating electric current flows mainly at the “skin” of the conductor
  • Due to “turbulent” eddy currents caused by changing magnetic field

• Stranding helps, but not as much as you might think
  • Touching surface area acts like single conductor
  • Individually-insulating strands (Litz wire) helps

• Coating with low-resistance material can leverage this property
  • E.g., silver-tinned copper
Improving Strength with Stranding

• **Solid vs Stranded conductors**
  - Solid: Inexpensive and tough, solid seating into jacks and insulation
  - Stranded: Increased flexibility and flex-fatigue life, increased conductivity

• **Stranding type affects wire properties**
  - **Bunched**: Inexpensive and simple to build, can be bulkier (circle packing problem)
  - **Concentric**:
    - Unilay: lighter weight and smaller diameter; greater torsional flex
    - Contra-helical: Greater mechanical strength and crush resistance; greater continuous flex
    - More twists → improve strength

• Ethernet comes in both solid (plenum and static runs) and stranded (standard, patch panel, etc)
Noise, Jamming, and Information Leakage

- When you move a conductor through a magnetic field, electric current is induced (electromagnetic induction)
  - EMI is produced from other wires, devices
  - Induces current fluctuations in conductor
  - Problem: crosstalk, conducting noise to equipment, etc
Reducing Noise with Shielding

- Enclose insulated conductor with an additional conductive layer (shield)
  - Reflect, absorb (Faraday cage), or conduct EMF to ground

- Types of shielding
  - Metallic foil vs. Braid shield
    - Foil is cheaper but poorer flex lifetime
    - Braid for low freq and EMI, Foil for high freq and RFI
    - Foil widely used in commodity Ethernet
    - Combining foil+braid gives best shielding
Reducing noise with Twisted Pairing

- Differential signaling: transmit complementary signals on two different wires
  - Noise tends to affect both wires together, doesn’t change relative difference between signals
  - Receiver reads information as difference between wires
  - Part of Ethernet standard, Telegraph wires were first twisted pair
Reducing noise with Twisted Pairing

• Disadvantages:
  • EMI protection depends on pair twisting staying intact → stringent requirements for maximum pulling tension and minimum bend radius (bonded TP can help)
  • Twisted pairs in cable often have different # of twists per meter → color defects and ghosting on video (CCTV)
Cable Ratings

• **Plenum rated** (toughest rating)
  - National Fire Protection Standard (NFPA) 90A
  - Jacketed with fire-retardant plastic (either low-smoke PVC or FEP)
  - Cables include rope or polymer filament with high tensile strength, helping to support weight of dangling cables
  - Solid cable instead of stranded
  - Restrictions on chemicals for manufacture of sheath → reduced flexibility, higher bend radius, and higher cost

• **Riser cable**: cable that rises between floors in non-plenum areas

• **Low smoke zero halogen**: eliminates toxic gases when burning, for enclosed areas with poor ventilation or around sensitive equipment
Physical Tapping

• Conductive Taps
  • Form conductive connection with cable

• Inductive Taps
  • Passively read signal from EM induction
  • No need for any direct physical connection
  • Harder to detect
  • Harder to do with non-electric conductors (e.g., fiber optics)
Tapping Cable: Countermeasures

• Physical inspection
• Physical protection
  • E.g., encase cable in pressurized gas
• Use faster bitrate
• Monitor electrical properties of cable
  • TDR: sort of like a hard-wired radar
  • Power monitoring, spectrum analysis
  • More on this later in this lecture
Case Study: Submarine Cable (Ivy Bells)

- 1970: US learned of USSR undersea cable
  - Connected Soviet naval base to fleet headquarters
- Joint US Navy, NSA, CIA operation to tap cable in 1971
- Saturation divers installed a 3-foot long tapping device
  - Coil-based design, wrapped around cable to register signals by induction
  - Signals recorded on tapes that were collected at regular intervals
  - Communication on cable was unencrypted
  - Recording tapes collected by divers monthly
Case Study: Submarine Cable (Ivy Bells)

- 1972: Bell Labs develops next-gen tapping device
  - 20 feet long, 6 tons, nuclear power source
  - Enabled

- No detection for over a decade
  - Compromise to Soviets by Robert Pelton, former employee of NSA

- Cable-tapping operations continue
  - Tapping expanded into Pacific ocean (1980) and Mediterranean (1985)
  - USS Parche refitted to accommodate tapping equipment, presidential commendations every year from 1994-97
  - Continues in operation to today, but targets since 1990 remain classified
Locating Anomalies with Time-Domain Reflectometry (TDR)

• A tool that can detect and localize variations in a cable
  • Deformations, cuts, splice taps, crushed cable, termination points, sloppy installations, etc.
  • Anything that changes impedance

• Main idea: send pulse down wire and measure reflections
  • Delay of reflection localizes location of anomaly
  • Structure of reflection gives information about type of anomaly
Motivation: Wave Pulse on a String
Motivation: Wave Pulse on a String

No termination

Reflection from soft boundary

Reflection from hard boundary

High to low speed (impedance)

Low to high speed (impedance)
TDR Examples

Melted cable (electrical short)

TDR: Inverted reflection

Cut cable (electrical open)

TDR: Reflection
TDR Example: Cable Moisture

Water-soaked/flooded cable

A Look inside Verizon's Flooded Communications Hub

Several floors of Verizon's headquarters are flooded at 140 West St. in Manhattan.

Eleven years after the 9/11 terrorist attacks, Verizon Communications Inc. is once again scrambling to repair severe damage to a key switching facility inside its historic headquarters building in lower Manhattan.
TDR Examples

Faulty Amplifier

Wire Tap
Protection against wildlife

Rodents

Moths

Cicadas

Ants

Crows
Protection against wildlife

- Rodents (squirrels, rats, mice, gophers)
  - Chew on cables to grind foreteeth to maintain proper length
- Insects (cicadas, ants, roaches, moths)
  - Mistake cable for plants, burrow into it for egg laying/larvae
  - Ants invade closures and chew cable and fiber
- Birds (crows, woodpeckers)
  - Mistake cable for twigs, used to build nests
- Underground cables affected mainly by rats/termites, aerial cables by rodents/moths, drop cables by crows, closures by ants
Countermeasures against wildlife

- Use High Strength Sheath cable
  - PVC wrapping stainless steel sheath
  - Performance studies on cable (gnathodynameter)

- Cable wrap
  - Squirrel-proof covers: stainless steel mesh surrounded by PVC sheet

- Fill in gaps and holes
  - Silicone adhesive

- Use bad-tasting cord
  - PVC infused with irritants
  - Capsaicin: ingredient in pepper spray, irritant
  - Denatonium benzoate: most known bitter compound
Optical Networking
Why optical networks?

• Today’s long-haul networks are based on optical fiber
  • >50% of Internet traffic goes over fiber optics, and increasing
  • Optical is the best choice for high datarate, long-distance
Why is fiber better?

• Attenuation per unit length
  • Reasons for energy loss
    • copper: resistance, skin effect, radiation, coupling
    • fiber: internal scattering, imperfect total internal reflection
  • So fiber beats coax by about 2 orders of magnitude
    • e.g. 10 dB/km for thin coax at 50MHz, 0.15 dB/km \( l = 1550\text{nm} \) fiber

• Noise ingress and cross-talk
  • Copper couples to all nearby conductors
  • No similar ingress mechanism for fiber

• Ground-potential, galvanic isolation, lightning protection
  • Copper can be hard to handle and dangerous
  • No concerns for fiber
Why *not* fiber?

• Fiber beats all other technologies for speed and reach
• But fiber has its own problems
  • Harder to splice, repair, and need to handle carefully
• Regenerators and even amplifiers are problematic
  • More expensive to deploy than for copper
• Digital processing requires electronics
  • So need to convert back to electronics
  • Conversion is done with an *optical transceiver*
  • Optical transceivers are expensive
• Switching easier with electronics (but possible with photonics)
  • So pure fiber networks are topologically limited:
    • point-to-point
    • rings
## Optical vs Copper

<table>
<thead>
<tr>
<th>Feature</th>
<th>Copper</th>
<th>Optical</th>
<th>Winner?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>24 voice channels</td>
<td>32000 voice channels</td>
<td>Optical</td>
</tr>
<tr>
<td>Weight</td>
<td>heavier</td>
<td>1/8&lt;sup&gt;th&lt;/sup&gt; weight of copper</td>
<td>Optical</td>
</tr>
<tr>
<td>Pull pressure</td>
<td>Bends under pressure</td>
<td>Can withstand high pressure</td>
<td>Optical</td>
</tr>
<tr>
<td>Loss</td>
<td>30db/km (loses 94% sig strength per 100 meters)</td>
<td>0.3db/km (loses 3% signal strength per 100 meters)</td>
<td>Optical</td>
</tr>
<tr>
<td>Repeaters</td>
<td>Every 5km</td>
<td>Every 50km</td>
<td>Optical</td>
</tr>
<tr>
<td>EMI</td>
<td>Affected by, causes EMI</td>
<td>EMI-proof</td>
<td>Optical</td>
</tr>
<tr>
<td>Reliability</td>
<td>Conductivity affected by power surges, temperature changes, severe weather, moisture</td>
<td>Resilient to weather/power</td>
<td>Optical</td>
</tr>
<tr>
<td>Fire</td>
<td>Old/worn cables create hazards</td>
<td>Low hazard</td>
<td>Optical</td>
</tr>
<tr>
<td>Cost</td>
<td>Lower deployment cost</td>
<td>Lower operating/maint cost</td>
<td>Depends</td>
</tr>
<tr>
<td>Power usage</td>
<td>High</td>
<td>Low</td>
<td>Optical</td>
</tr>
<tr>
<td>Security</td>
<td>Easier to tap</td>
<td>Difficult to tap</td>
<td>Optical</td>
</tr>
<tr>
<td>Skill required</td>
<td>Low</td>
<td>High</td>
<td>Copper</td>
</tr>
<tr>
<td>Deployment</td>
<td>Widely entrenched</td>
<td>Upcoming</td>
<td>Copper</td>
</tr>
<tr>
<td>Equipment Cost</td>
<td>$15 SFP, $1.1 per meter cable</td>
<td>$20 SFP, $1.6 per meter cable</td>
<td>Copper</td>
</tr>
</tbody>
</table>
Main components of a fiber-optic network

- Fiber
- Light sources and receivers
- Amplifiers
- Couplers
- Modulator
- Multiplexor
- Switch
Optical Fibers

- Very pure and transparent silica glass
  - Jacket/buffer protects the rest of the fiber

- Core transmits light
  - Some fibers also use cladding to transmit light

- Cladding and core transmit light
  - Cladding has lower refractive index than core
  - Cladding causes light to be confined to the core of the fiber due to total internal reflection at the boundary between the two
    - Beyond critical angle, all light is reflected
  - Some fibers support cladding modes where light propagates in the cladding as well
    - Most fibers coat cladding with polymer with slightly higher refractive index, to rapidly attenuate light propagating in cladding
    - Exception: double-clad fiber, which supports a mode in both its cladding and its core
Inside an optical fiber

• **Refractive index** of core (n1) is bigger than that of the cladding (n2)
  • Done by doping core with impurity (eg Germanium Oxide)
  • Goal: cause light to be confined to the core due to **total internal reflection**
Keeping the light in the core with Total Internal Reflection

- **Case 1:** angle of incidence is **less** than the critical angle
  - \( \theta_i < \theta_c \)
  - \( \theta_c = \sin^{-1}(n_2/n_1) \) → All light is reflected
  - This really is 100% reflection – wouldn’t have such low-loss fibers otherwise

- **Case 2:** angle of incidence is **greater** than the critical angle
  - \( \theta_i > \theta_c \) → Some light is reflected, but some is also refracted
Acceptance angle

- Critical angle determines acceptance angle of light going in
  - Light received at too much of an angle will have high attenuation
  - Numerical aperture (NA): size of cone of light input that will be totally internally reflected
    - $\text{NA} = n_0 \sin (\Theta_0)$
Multiplexing Techniques

- **Wavelength Division Multiplexing (WDM)**
  - Different sources = different colors
- **Optical Time Division Multiplexing (OTDM)**
  - Different sources = different time slots
- **Optical Code Division Multiplexing (OCDM)**
  - Derive a set of orthogonal “codes”
  - Different sources = different codes
Single- vs. Multi-mode optical fiber

• Single-mode fiber is designed to carry a single “ray” (mode) of light

• Multi-mode fiber carries multiple rays/modes
  • Larger core than single mode
  • Higher loss, hence used over shorter distances (within a building or on a campus)
  • Typical rates of 10Mbit/s to 10Gbit/s of lengths up to 600 meters
Signal attenuation in optical fibers

• Fibers are much more efficient transmitters than copper wires
• Certain wavelengths have especially low loss
  • 1300 and 1500 μm → 0.1 dB/km (~2% per km loss) → very efficient
  • Very efficient due to total internal reflection
• Why is there any loss at all?
  • Why are certain wavelengths more affected by loss?
Why is there loss in optical fibers?

- Rayleigh scattering
- Material absorption
- Micro- and Macrobending
- Chromatic dispersion
Why is there loss in optical fibers?

• Rayleigh scattering
  • Light hits and bounces off particles (individual atoms or molecules)
  • Blue is scattered more than other colors, as it travels in smaller, shorter waves
  • Same reason sky is blue during day and red at night
  • Bigger effect at smaller wavelengths
Why is there loss in optical fibers?

• **Material absorption**
  • Intrinsic absorption in infrared and ultraviolet bands
  • Impurities in optical fibers
    • Most important one: water in the form of hydroxyl ions, causing losses at 950, 1250, and 1380 nm
Why is there loss in optical fibers?

• **Mechanical issues**
  • **Microbending**: Local distortions of fiber geometry/refractive index
  • **Macrobending**: excessive fiber curvature
    • Occurs when installing fiber
Macrobending example

- http://www.youtube.com/watch?v=1ex7uTQf4bQ
Chromatic dispersion

• Velocity of light is $3 \times 10^8$ m/s in vacuum
  • But in a transparent medium, phase velocity of light wave depends on its frequency
  • Red, which has longer wavelength than blue, will travel faster
  • In glass, red travels at 66.2% of $c$, blue travels at 65.4% of $c$
    • This is what causes rainbows
<table>
<thead>
<tr>
<th>Fiber Type</th>
<th>Wavelength</th>
<th>Fiber attenuation / km *</th>
<th>Fiber attenuation / km #</th>
<th>Connector Loss</th>
<th>Splice Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimode 50/125μm</td>
<td>850nm</td>
<td>3.5 dB</td>
<td>2.5 dB</td>
<td>0.75 dB</td>
<td>0.1 dB</td>
</tr>
<tr>
<td></td>
<td>1300nm</td>
<td>1.5 dB</td>
<td>0.8 dB</td>
<td>0.75 dB</td>
<td>0.1 dB</td>
</tr>
<tr>
<td>Multimode 62.5/125μm</td>
<td>850nm</td>
<td>3.5 dB</td>
<td>3.0 dB</td>
<td>0.75 dB</td>
<td>0.1 dB</td>
</tr>
<tr>
<td></td>
<td>1300nm</td>
<td>1.5 dB</td>
<td>0.7 dB</td>
<td>0.75 dB</td>
<td>0.1 dB</td>
</tr>
<tr>
<td>Single Mode 9μm</td>
<td>1310nm</td>
<td>0.4 dB</td>
<td>0.35 dB</td>
<td>0.75 dB</td>
<td>0.1 dB</td>
</tr>
<tr>
<td>Single Mode 9μm</td>
<td>1550nm</td>
<td>0.3 dB</td>
<td>0.22 dB</td>
<td>0.75 dB</td>
<td>0.1 dB</td>
</tr>
</tbody>
</table>

*These values are per TIA/EIA and other industry specifications and are the values used by Transition Networks in all link loss calculations.

#These values are one example of the performance that can be obtained with a new fiber installation.
Laying Fiber

• How to lay cable over long distances?
  • Rail lines sell easements to permit laying of cable along rail line right-of-ways
  • Digging up and laying is the expensive part
    • So, lay extra fiber and leave it dark (“dark fiber”)
    • Light it up when more capacity needed
Optical components

- Transmitter/receiver
- Optical amplifier
- Optical coupler/splitter
- Optical delay units (packet buffering)
Optical transmitters/receivers

• Transmitting light with lasers
  • Laser diodes: created by doping thin layer on crystal wafer to create a p-n junction
  • Fiber Laser: Gain medium (doped optical fiber) amplifies beam through spontaneous emission

• Receiving light with photodetectors
  • Inverted diode: apply reverse voltage across p-n junction, light excites current
Optical Amplifiers

• Amplifies optical signal without converting it to electricity
• Doped Fiber Amplifier: signal is amplified through interaction with doping ions
• Used to correct attenuation
  • Placed every 100km on long-haul links
Optical Coupler/Splitter

• **Splitter**: The optical version of a copying machine
  • Divides one incoming signal into multiple signals
  • Made from half-silvered mirror, or two joined prisms
  • Adjusted so that half of light is reflected and other half is refracted
• **Coupler**: joins two signals

• Uses:
  • Getting two copies of a signal (wiretapping)
Optical Networks: Resilience and Security
Service Disruption Attacks

- Goal: cause delay, service denial, QoS degradation, spoofing
- Can easily cut/disrupt optical fiber
- Can bend fiber to radiate light in/out of fiber
- In-band Jamming
  - Attacker injects signal to confound receiver
  - Signals flow through nodes without electrical regeneration → attack can easily spread through network
Service Disruption Attacks

• Out-of-band jamming: attacker jams signal by exploiting leaky components
  • Exploits crosstalk in various components

• Examples
  • Attacker can hop wavelengths by sending very strong signal
    • WSSs can have crosstalk levels of -20dB to -30dB
  • Inject signal on different wavelength but within amplifier passband
    • Gain for comm signal is robbed by the attack signal
  • Electromagnetic Pulses (EMP) could cause both in-band and out-of-band jamming
Tapping Attacks

• Contemporary demultiplexers exhibit crosstalk levels of 0.03% to 1%
  • Leak a little bit of the signal on the wrong path, attacker can listen in
• Fibers can leak across wavelengths due to chromatic dispersion
• Optical amplifiers can leak due to gain competition
  • Attacker can co-propagate a signal on a fiber and observing cross-modulation effects
• Tapping can be combined with jamming
  • Tap, and inject a correlated signal downstream of the tap point
  • Very harmful to users with low SNR
Mitigating Attacks on Optical Networks

• Optical Limiting Amplifier: limits output power to specified maximum
  • Limiting light power limits crosstalk and service disruption attacks

• Band-Limiting Filters: discard signals outside a certain bandwidth
  • Can prevent gain competition in optical amplifiers
Mitigating Attacks on Optical Networks

• Physically strengthen or armor the cladding
  • Bury cable in concrete, enclose cable in pressurized pipe
  • Usually very expensive

• Choose devices with lower crosstalk

• Choose more robust transmission schemes
  • Coding to protect against jamming
  • Intelligent limiting of signals to certain bandwidths/power constraints

• Architectural techniques
  • Avoid easily-compromised links for sensitive communications
  • Judicious wavelength assignment to separate trusted from non-trusted users
Detecting Attacks

• Power detection: compare received optical power to expected optical power
  • Too much: jamming attack?
  • Too little: tapping?
  • Challenges: slight changes are difficult to detect; small but detectable changes result from component aging and fiber repairs. Tuning problem.
  • Sporadic jamming might harm BER but might not change power levels enough to show up
Detecting Attacks

• Optical spectrum analysis: measure spectrum of optical signal
  • Can help localize gain competition attacks
  • Require additional processing time and hence can slow detection time

• Pilot tone: known signal, different carrier frequency, but traveling on same path as data
  • Used to detect transmission disruption
Detecting Attacks

• Optical TDR: like pilot tones, but analyze echo
  • Used to detect attacks involving fiber tampering, e.g. in-line eavesdropping
  • Challenge: EDFAs are sometimes unidirectional, not reflecting the echo
    • May require bi-directional amplification
Collision Detection (wired)
Collision Detection (wired)