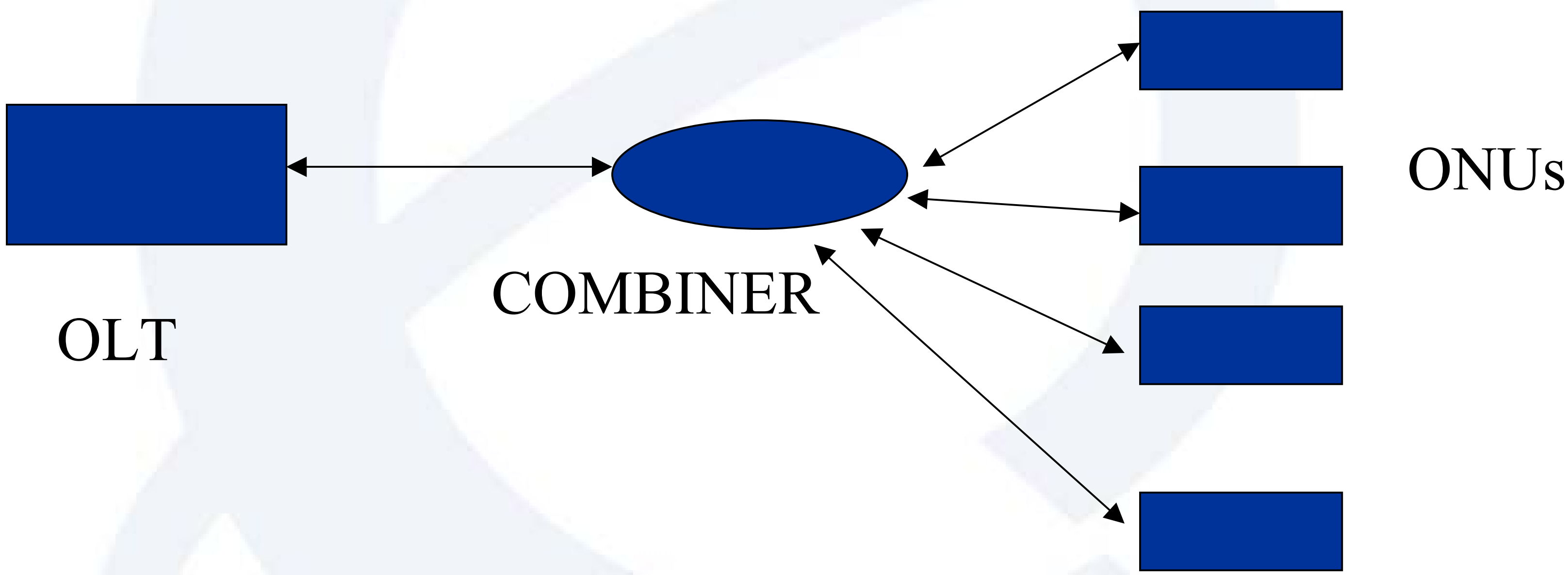
Physics arguments for upstream encryption in PONs

Marcus Leech

Advisor, Security Engineering

Nortel Networks

xPON architecture



xPON risks in the upstream

- **Combiners have variable directivity**
  - 30-50dB common
  - another 15db of path loss for a 32 port combiner
- **ONU output power varies from -5dBm to -12dBm**
- **Newer off-the-shelf APD receivers have typical sensitivities down to -40dBm for 10e-12 BER**
- **Within “reasonable” for OTS receiver**
- **Simple cooling of the APD improves sensitivity dramatically. SINGLE PHOTON detection using InGaAs APD and TEC has been regularly demonstrated over the last several years.**

xPON upstream: Scenario 1

- **30 subscribers on combiner**
  - 14.7dB attenuation
- **Cheap combiner**
  - 30dB effective attenuation
- **Powerful transmitter**
  - -5dBm
- **Signal arrives at “bad” guy at -50dBm**
  - within 10-15dB of detection for current APD receiver at room temperature (depending on BER tolerance of our bad guy)
  - probably detectable using modest cooling techniques
    - peltier devices
    - stick receiver in the deep freeze in the basement

xPON Upstream: Scenario 2

- **Bad splice on OLT side of combiner**
  - very common occurance: -3dB (50%) to -10dB (10%) reflectance
    - not bad enough to affect normal operations
    - link margins usually quite high, no reason to replace bad splice
      - costs money to fix splice that has almost no impact on BER
- **Calculation**
  - -10dB from splice
  - -11dBm from ONU
  - -5dB fiber attenuation (0.5dB/Km @ 10 km)
  - 15dB for 32:1 combiner
- **Signal arrives at “bad guy” at -40dBm to -45dBm**
  - easily within detection threshold

Basic detector physics

- **Noise Equivalent Power**
  - input power level required to produce 1:1 SNR at device output
  - defined as watts/sqrt(hz bandwidth)
  - NEP of 1.0e-15W/sqrt(BW) for low noise silicon photodiodes achievable
- **NEP consists of thermal noise (Ij):**
  - Ij = sqrt(4kTBF/Rsh)
    - k Boltzmanns constant (1.38e-23 joules/K)
    - B noise bandwidth
    - T absolute temperature (IMPORTANT--reduce temperature, reduce thermal noise!)
- **divided by Radiant Sensitivity (A/W)**
- **At low signal levels, SNR is dominated by thermal noise of the device.**

Detector physics: example

- **Assume detector with NEP of 9.9e-15 W/sqrt(BW)**
  - (Ref: HAMAMATSU S2386-33BR Pin Photodiode)
- **Assume simple (NRZ) modulation of 155mbit signal**
- **Define bandwidth to be 2.5 x bitrate = 388MHZ**
- **Total noise power is:**
  - 9.9e-15 * sqrt(3.88e8)
  - -67.0 dBm noise power
- **10dB SNR requires signal at -57dBm or better**
- **If willing to tolerate high BER (the bad guy IS willing to tolerate high BER!!), then only a few dB SNR required**
- **Improved NEP (by 2-3dB) can be achieved by cooling**

Signal detection strategies

- Higher path loss simply reduces BER
- OTS receivers specified at 10e-12 BER for given input power levels
- Bad guy willing to tolerate poorer BER, even by several orders of magnitude (10e-8 rather than 10e-12, for example).
- Diversity reception (multiple legitimate subscriptions) can improve detection by 3dB for every doubling. Have to deal with clock skew, but at modest bit rates, not hard.

Conclusions

- **Encryption of UPSTREAM essential**
  - within 10-15dB of “disaster” under ideal circumstances
  - minimal magic required if bad splice on OLT side of distribution network
- **Reliance on transient physical properties very risky proposition**
  - advances in single-photon detection moving forward very rapidly using InGaAs APD detectors. No reason to expect such advances not to map into optical network receivers.
  - Problems that are only within 1 or 2 orders of magnitude of being solved make cryptographers and security people very nervous.

References

- **OTS APD receivers:**
  - OCP SRX-12-APD receiver
    - -40.5dBm typical sensitivity for BER of 10e-10 at 622Mbit
  - AGERE RA194W
    - -26dBm typical sensitivity for BER of 10e-12 at 10gbit
  - OPTOCOM OPT1275
    - -41dBm typical sensitivity for BER of 10e-13 at 622Mbit
  - OKI AAR1525 LV
    - -44dBm typical sensitivity for BER of 10e-11 at 155Mbit
- **Single photon detection**
  - “Secure Optical Cryptography Moves Closer to Reality”
    - article on optics.org
  - “A 1550nm single-photon detector using a thermoelectrically cooled InGaAs avalanche photodiode” Yoshizawa A., Tsuchida H. Japanese Journal of Applied Physics, Vol 40, Issue 1.