EPON Properties for Security

Onn Haran, Passave

Motivation

- EPON has some specific properties which might be utilized for security
- Security solution could be much simpler when considering these properties

MPCP Clock Synchronization

- **MPCP system is synchronized**
  - Packet transmitted from OLT at time T is received by ONU at time T
  - Packet transmitted from ONU at time T is received by OLT at time T+RTT
- **PON clock value can be used for**
  - Initialization Vector (IV) synchronization
  - Replacing replay counter

Virtual Point-to-point Link

- Point to point emulation defines a virtual link between OLT and each ONU
- A link is identified by LLID tag
- The same LLID tag can be used as SAID (Security Association IDentifier)

No Man-in-the-middle

- **Extremely low probability for existence of an entity that terminates a packet, modifies it, and returns it to the line as it was not modified**
- **Message authentication can be based on encrypting FCS instead of adding HMAC**
  - It is extremely difficult to fake valid encrypted FCS without knowing the encryption key
  - It is relatively easy to modify an encrypted packet keeping a valid FCS → Non issue without man-in-the-middle attack

Required Indications

- Packet is encrypted – 1 bit
- Sequence number of used key – 1 / 2 bits
- PON clock wrap around – 1 bit
- Key acknowledge – 0 / 1 bit

Conclusion

- **Encryption header based on presented properties can be 1 byte**
  - No need for 4-8 bytes of message authentication
  - No need for 3 bytes for initialization vector
  - No need for 2-4 bytes for SAID