Security threats and mechanisms

Ajay Gummalla, Broadcom
Carlos Ribeiro, CTBC Telecom
Charles Cook, Qwest
Glen Kramer, Alloptic
Olli-Pekka Hiironen, Harald Kaaja, Nokia
Onn Haran, Passave

Scope

- Security threats
- Security mechanisms
- What can be done in 802.3 scope?

Security threats

- Eavesdropping
- Impersonation
- Denial of service

Eavesdropping

- User can monitor all downlink traffic
  - Using a standard sniffer
- It is difficult to monitor uplink traffic
  - Neighbor in the same PON:
    - Requires isolation of reflected uplink wavelength using a filter
    - Depends on network topology
  - Unauthorized connection to splitters is possible and easy, though illegal…

Impersonation

- ONU may be compromised
- User may learn MAC addresses of all stations within PON
- User sends data to the network as another user
  - User in the same PON
- User sends data as a management entity
  - User can reside either inside or outside the PON
- More dangerous when peer-to-peer is enabled

Denial of service

- User floods the network with either valid or invalid data
  - User can reside either inside or outside the PON
- Malicious user can deny service to a specific user

Scope

- Security threats
- Security mechanisms
- What can be done in 802.3 scope

Encryption

- Encrypting downlink data protects against eavesdropping
- Encrypting uplink data protects against unauthorized connections to splits and limits PON internal impersonation
- Encrypting MAC address decreases risks from compromised ONU and impersonations
- Encryption should be based on a strong algorithm (AES is recommended)

Access authentication

- Authentication validates user identity
- Authentication occurs after registration
- Prior to authentication, ONU data traffic is disabled
- 802.1x specifies a framework for authentication – further study is required

Source monitoring

- Control messages must contain valid source
  - Identification based on only MAC source address is not enough
- Packet from suspicious source can be discarded based on port

Upper layers security

- Security can be implemented in several layers simultaneously
- Security should be part of EFM because:
  - Upper layers aren't aware that PON is unsecured
  - Every PON user must know that PON isn’t safe and should configure IPsec
  - PON created the security problem → PON should solve this problem

What can be done in 802.3 scope?

- Security solution must be limited to minimal augmentation of PHY and MAC operation
- Downlink and uplink encryption should be added
- Other security mechanisms will not be standardized but should be included in high layer implementation