Security Threats and Defense Models in EPON

Olli-Pekka Hiironen and Antti Pietiläinen, Nokia

Security threats in P2MP
(SEVERITY)

- **PON medium is broadcast in downstream (VERY HIGH)**
  - Every ONU located in end-users' premises can eavesdrop downstream traffic unnoticed and undisturbed 24h/day using a standard Gb Ethernet interface.
  - The attacker can know the MAC addresses and LLIDs used by neighbors.
  - The attacker could infer the amount and type of traffic to neighbors by monitoring LLIDs and Ethernet MAC addresses.
  - Downstream MPCP messages can reveal upstream traffic characteristics of each ONU.

Security threats in P2MP
(SEVERITY)

- **PON medium is multi-point-to-point in upstream (HIGH)**
  - The attacker can masquerade as another ONU (using MAC address and/or LLID) and gain access to privileged data and resources in the network.
  - The attacker can steal the service by overwriting the signal with higher power. 6dB-10dB higher power is enough.
  - The intruder can flood the network with either valid or invalid messages affecting the availability of the network resources or OAM information, e.g. counters in OLT.
  - If the intruders succeed to hack into OAM channels, they can try to change EPON system configurations or get access to TMN network.
  - End user may try to disturb the PON by sending any optical signals upstream (e.g. signal from standard Ethernet long wavelength interface). This could generate restarts which may ease hacking the protection mechanisms.

Security threats in P2MP
(SEVERITY)

- **PON medium may have high discrete reflections (LOW - MEDIUM)**
  - Upstream traffic of one ONU may be detectable from other ONU access points.
  - The attacker could intercept upstream frames by using reflections from PON, modify frames, and send them to OLT.

Threat model in P2MP

- **PON medium is broadcast in downstream**
  - Confidentiality
  - Privacy
- **PON medium is multi-point-to-point in upstream**
  - Authentication
  - Access control
  - Data origin authentication
  - Denial of service prevention
- **PON medium may have high discrete reflections**
  - Data integrity

Security objectives in P2MP
(IMPORTANCE)

- **Confidentiality (MUST):** Keeping information secret from all but those who are authorized to see it

- **Authentication (MUST):** The network wants to be sure about ONU’s identity

- **Access control (MUST):** Network wants to control the access of ONU's to network resources.

- **Message authentication (data origin authentication) (MUST):** A type of authentication whereby a party which receives a message have assurance of the identity of the party which originated the message

- **Data integrity (MUST):** The receiver wants to be sure that the received message has not been modified

- **Privacy (IMPORTANT):** It is not possible to infer confidential data by passive attacks, e.g. analysis of traffic volume or destination

Security objectives in P2MP
(IMPORTANCE)

- **Denial of service prevention (IMPORTANT):** Enemies can neither prevent the use of any resources to legitimate users nor decrease system performances

- **Non-repudiation of origin (WISH):** The sender can not deny that he sent a message

- **Non-repudiation of delivery (WISH):** The receiver can not deny that he received the message

Defense model

- Confidentiality
  - Encrypt data messages.
- Privacy
  - Encrypt MAC addresses
- Authentication
  - Authentication
- Access control
  - Access control
- Data origin authentication
  - Message authentication
- Denial of service prevention
  - Message authentication, fix auto-discovery problems,...
- Data integrity
  - Integrity protection

Encryption is required for confidentiality

- A long key, 128 bits or more, should be used.
- New keys should be distributed through encrypted channel.
- Any two packets should be encrypted with a different key. If a new key would be distributed for every packet, too much overhead would be generated. Therefore, an initialization vector is necessary. The original value of the initialization vector and its variation from packet to packet is known by the endpoints. The initialization vector and the distributed key are combined to produce a new key for every packet.
- It is possible that a packet is lost and the receiver would loose track of the correct initialization vector. Therefore, it may be required that about one bit is used to indicate the sequence number.
- New key should be distributed once a while.

Requirements (Downstream)

		Security mechanisms					Req. in EPON
Security objectives	Severity * probability	Authentication	Encryption	Mess. Auth.	Data integrity	Digital signature	
Confidentiality	very high		x				yes
Authentication	low	x					no
Message authentication	low	x		x			no
Data integrity	low	x			x		no
Access control	low	x		x			no
Privacy	high		x				yes
Non-repudiation of delivery	moderate	x			x	x	?
Denial of service prevention	low						no
requirement in EPON		no (?)	yes	no	no (?)	?	

Requirements (Upstream)

Security objectives in EPON	Severity * probability	Security mechanisms in EPON					Req. in EPON
		Authentication	Encryption	Mess. Auth.	Data Integrity	Digital Signature	
Confidentiality	low – mod.		x				maybe
Authentication	very high	x					yes
Message authentication	high	x		x			yes
Data integrity	low – mod.	x			x		maybe
Access control	high	x		x			yes
Privacy	low – mod.		x				maybe
Non-repudiation of delivery	moderate	x			x	x	?
Denial of service prevention	high						?
Requirement in EPON		yes	maybe	yes	maybe	?	