An EPON Security Proposal

– Churning and Password Mechanism adapted from APON

Chan Kim, Tae Whan Yoo

ETRI

ETRI

Security requirements

- Security is strongly needed in EPON public access network for many reasons as revealed in hiironen_1_0502.pdf
- downstream data should be protected so that other ONUs cannot “listen” to the sensitive data destined to a specific ONU
- OLT should be able to check whether the ONU that it is talking to is the registered, ligitimate ONU
- Is higher layer encryption enough ? => No, because not every application use encryption, and because it’s now public PON.

ETRI

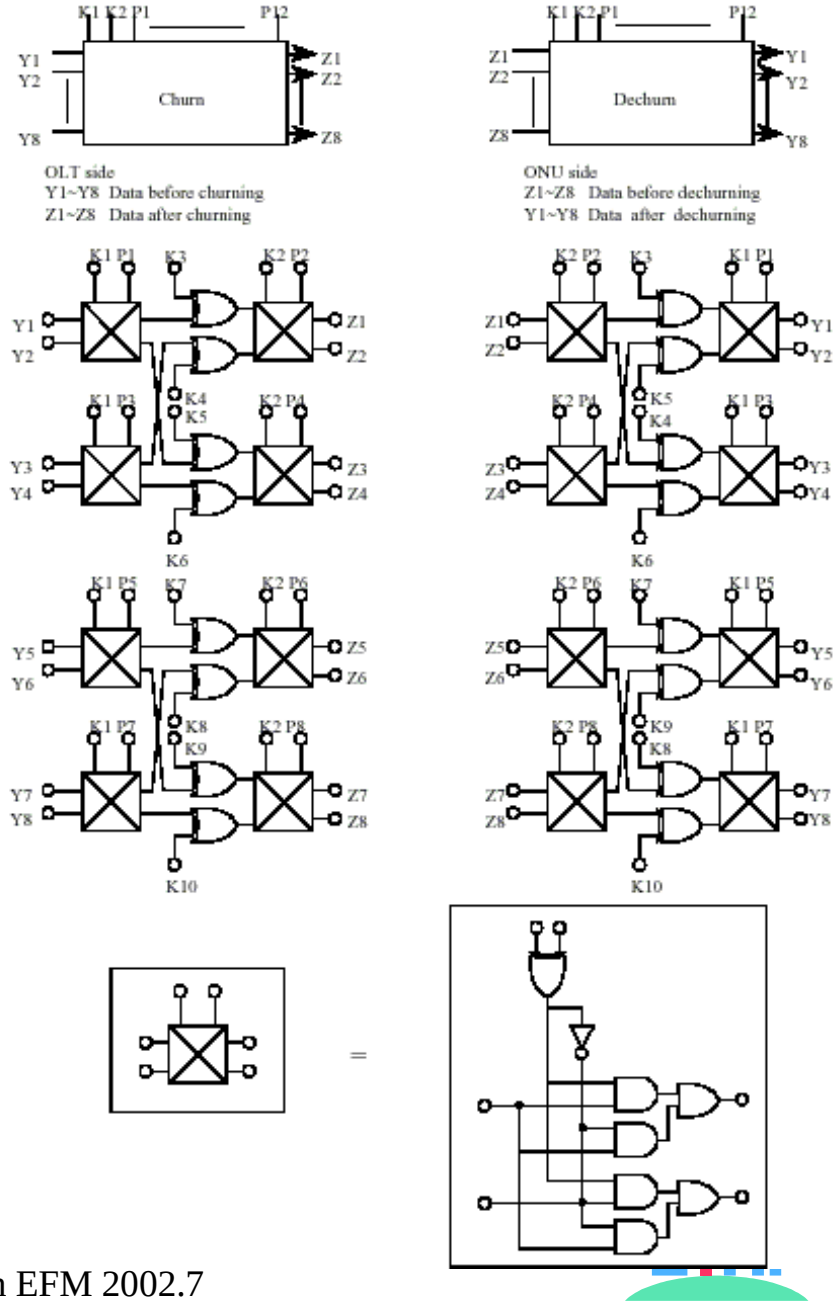
Security Functions

- Why define a new one when we already have a very similar function in ATM-PON?
- Security in EPON can be achieved using methods used in APON
  - downstream data privacy => using simple churning mechanism
  - ONU authentication => using password mechanism
  - deactivating an ONU => using special message
- MPCP messages should be added for above functions

ETRI

Churning

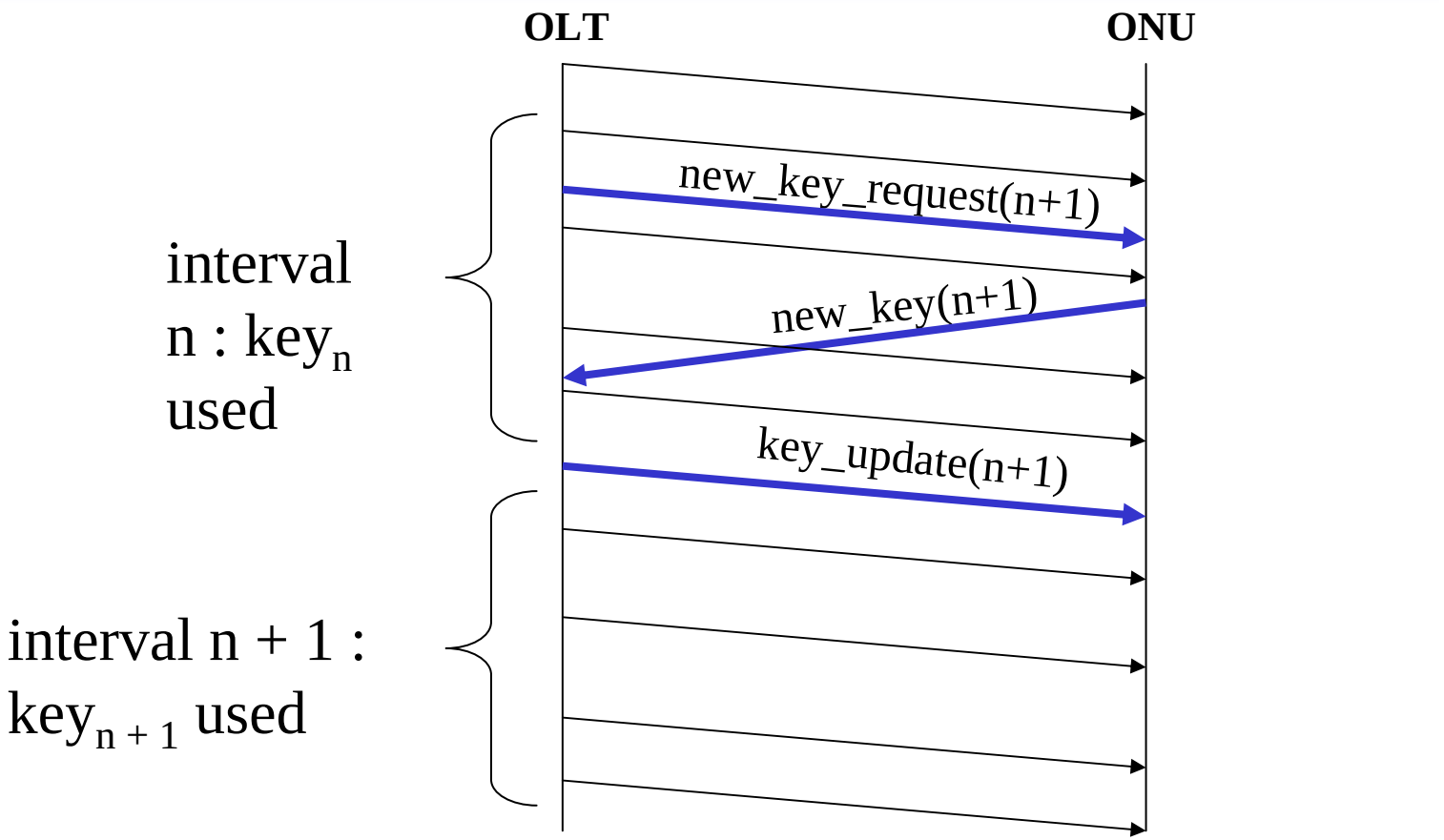
- defined in G.983.1
- 3 byte churning key needed for each ONU
- churning key updated frequently by OLT request and generated by ONU
- downstream data is churned using different churning keys for each ONU



Messages for churning

- New_Key_Request (OLT->ONU) : requests a new key for an ONU. includes the key sequence number which runs from 0 to 255.
- New_Key (ONU->OLT) : carries new key generated at the ONU together with the key sequence number. the new key will be used for the next key update
- New_Key_Update(OLT->ONU) : lets the ONU know that the newly generated key should be used afterwards which has been kept in the ONU. It carries the key sequence number also.
- Using the key number, no acknowledgement is necessary in case the New_Key message was not delivered correctly to OLT before.

Churning Key Update Timing



* Message and packets shown only for one ONU

And to be more specific,

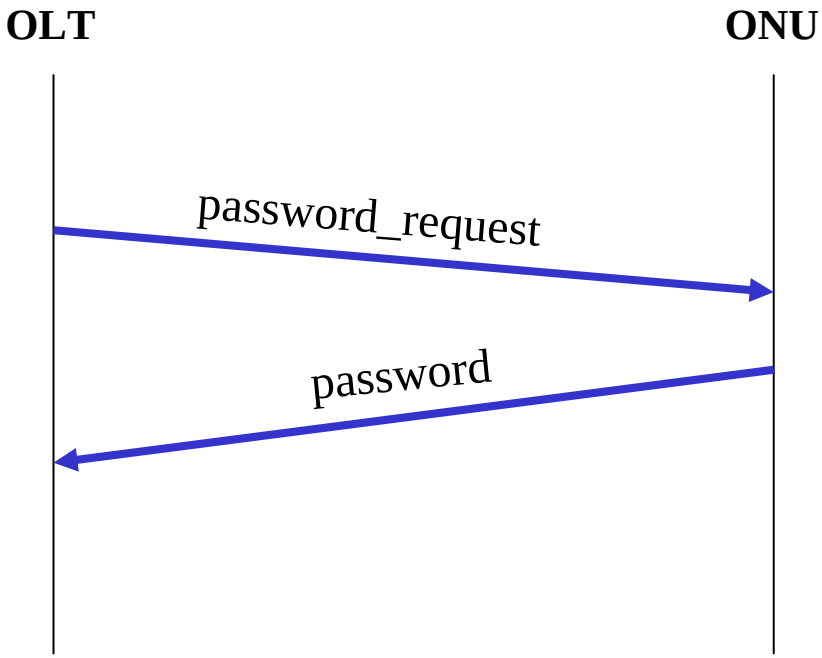
- Layer : between MAC and RS
  - can be incorporated into a “PON adaptation” sub-layer
  - Churning information delivered in the preamble
- One key and one LLID for one ONU
  - LLID doesn’t have any meaning end-to-end, it’s PON specific, devised for bridge compliance handling
  - Reduce the scheduling burden in OLT,ONU
- Encrypt the whole frame but only those sent downstream in P2PE mode
  - No churning key problem for Multicast/Broadcast frames
  - No churning key problem for SCB, anti-LLID frames
  - The “PON adaptation” sub-layer generates/receives preamble and handles churning processing together

ETRI

Password mechanism

- Since all the MAC addresses of the ONUs can be extracted from downstream data, a malicious user can masquerade another ONU (after cutting the fiber?)
- To counteract this, the OLT may request the password of the ONU. This password is only sent in upstream direction and cannot be recovered by other connected ONUs.

Password



* for one ONU

Conclusion

- downstream privacy through churning mechanism
  - “PON adaptation” layer between MAC and RS
  - One key, one LLID per one ONU. That’s simple and enough
  - Churn the whole frame sent downstream in P2PE mode (but not in anti-LLID mode) => solves multicast problems
- ONU authentication using password mechanism
- Define “deactivate ONU” message in MPCP
- Proposed schemes are simple, easy to implement, but provides enough confidentiality