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

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 authentification => using password mechanism
  - deactivating an ONU => using special message
- MPCP messages should be added for above functions

ETRI

Downstream privacy : Churning

- Used in ATM-PON, defined in ITU-T G.983.1
- definition in APON specification :
  - Churning is a function which can be applied to the downstream user data from an OLT to its ONUs. Churning provides the necessary function of data scrambling and offers a low level of protection for data confidentiality It is installed at TC layer and can be activated for point-to-point downstream connections
- Can be implemented in MAC layer in EPON or in separate layer.(it's not important in real implementaion what layer it is located)

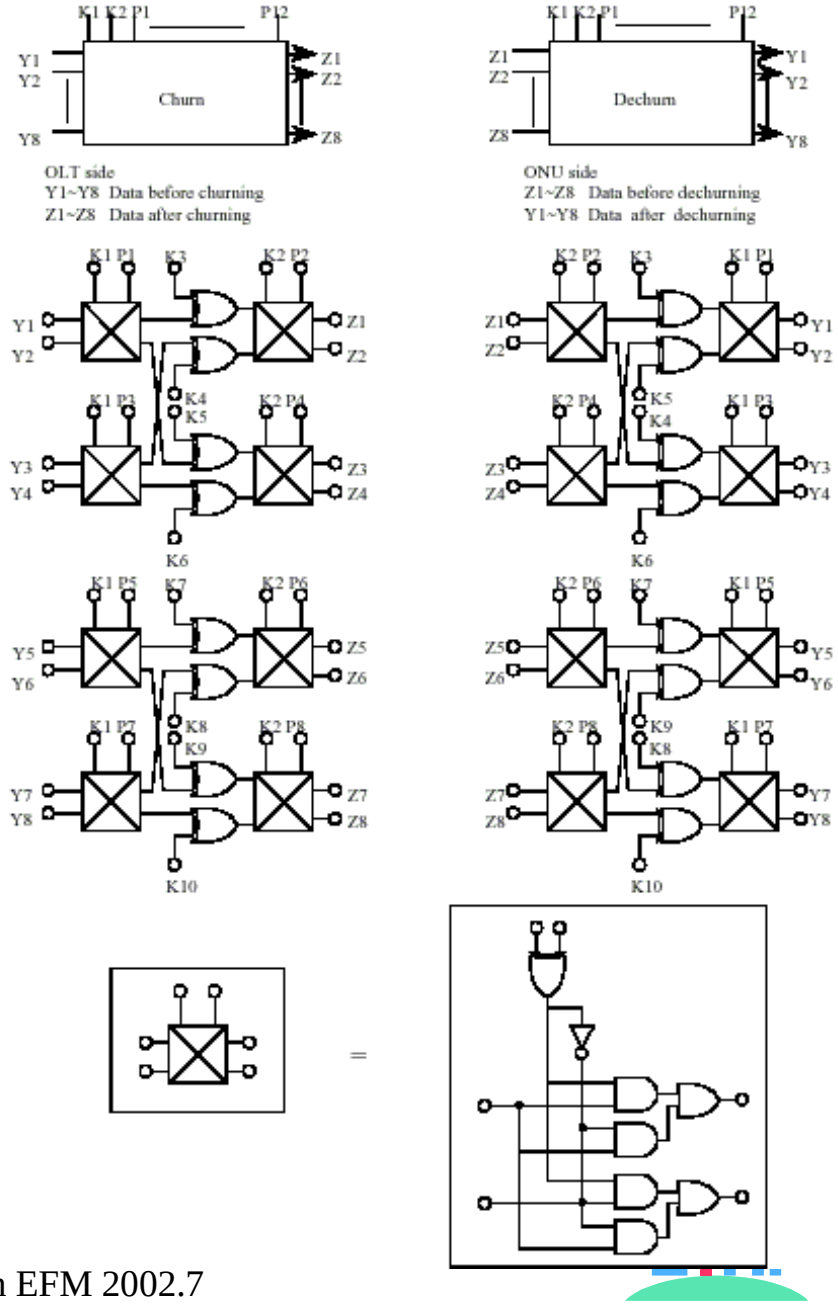
Churning(cont.)

- encrypt the downstream data using different keys for each ONU
- For each ONU, on OLT's request, churning key is generated by the ONU and sent upstream to OLT so that the OLT can churn the downstream data with different key for each ONU
  - XOR of random number and upstream data is used as churning key for robustness
- Churning key is updated frequently and key update is synchronized between OLT and ONU using message
- Some traffic may be better not to be churned (ex. video broadcast)
  - churning should be enabled/disable on frame by frame bases
  - enable/disable information should be coming down from upper layer through system level interface, but the mechanism to send the enable/disable information should be provided in the frame

ETRI

Churning

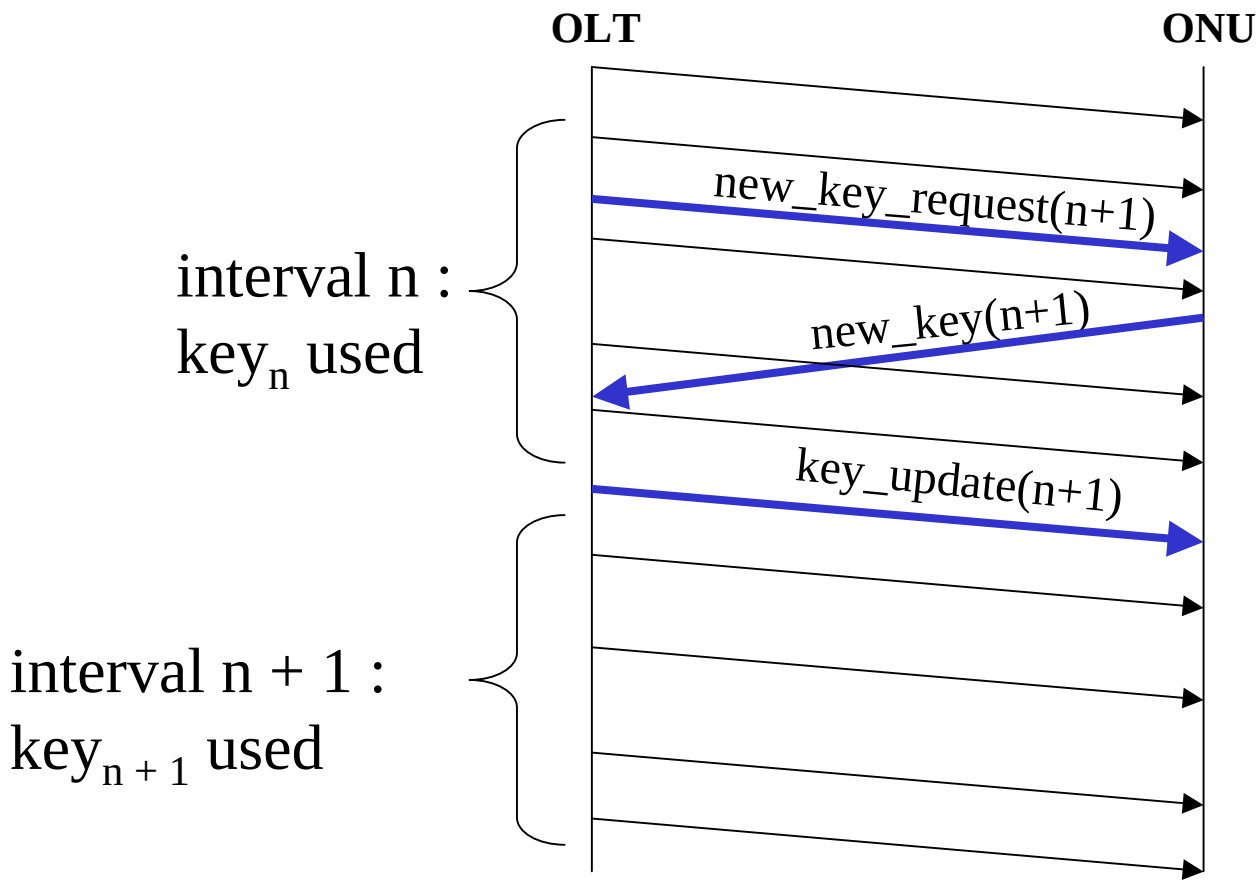
- defined in G.983.1
- 3 byte churning key needed for each ONU
- churning key updated frequently by OLT request and generated by ONU
- downstream data is churned using different churning keys for each ONU



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.

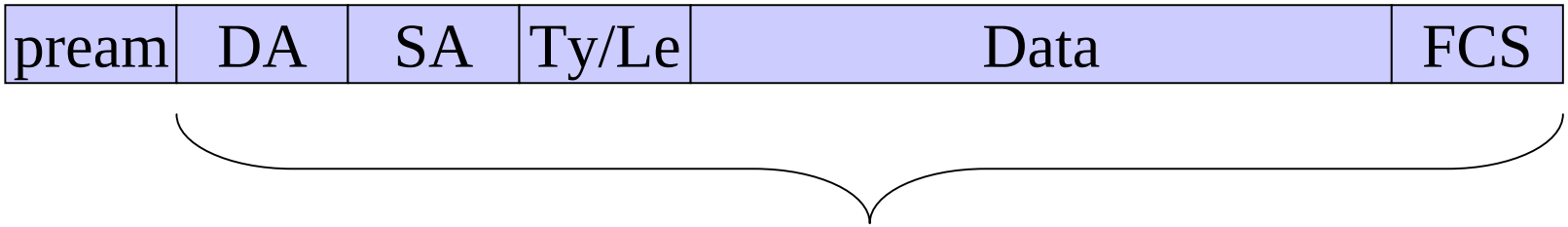
Churning Key Update Timing



* Message and packets shown only for one ONU

What portion to churn?

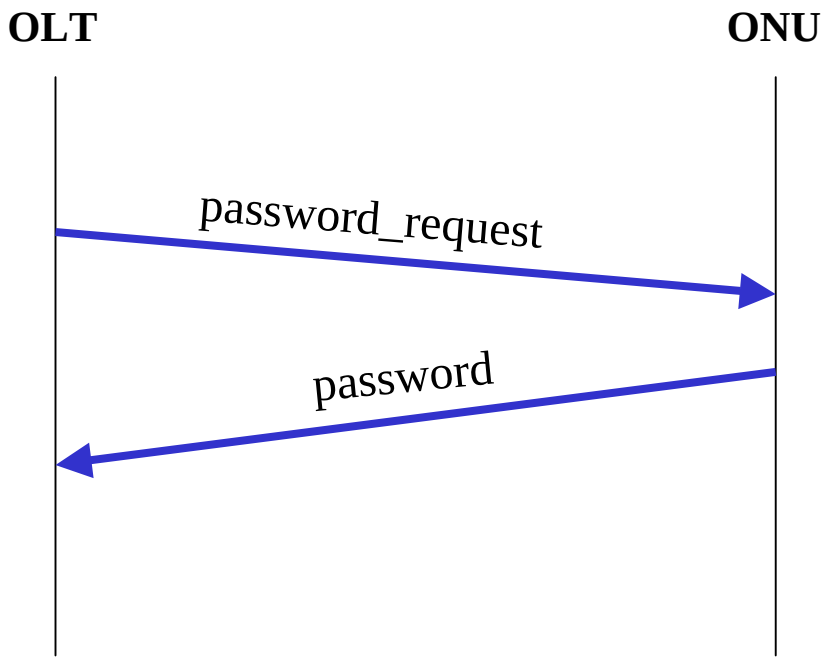
- Choice 1 : from DA to FCS, all frames
- Choice 2 : from DA to FCS, all frames except MPCP frames for safety
- There is no problem in FCS handling
  - in OLT, FCS is generated after churning
  - in ONU, FCS is analyzed before churning
  - FCS errored frames are discarded



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 thrugh churning mechanism
- ONU authentication using password mechanism
- Both are simple, and were adapted from APON