Security baseline proposal

Antti Pietiläinen
Ariel Maislos
Glen Kramer
Olli-Pekka Hiironen
Onn Haran

Security objectives requiring work in EFM

- Confidentiality
  - Every ONU located in end-users' premises can eavesdrop downstream traffic unnoticed and undisturbed 24h/day
  - OAM frames can contain confidential information
  - Upstream traffic can theoretically be seen by other ONUs if reflections from PON are too high

  ⇒ **Payload should be encrypted in up- and downstream**
- Message Authentication
  - The attacker could masquerade in the upstream as another ONU and gain access to privileged data and resources in the network.

  ⇒ **Message authentication should be guaranteed in upstream. It can be based on encryption of frame including CRC in upstream and checking correctness of the decrypted CRC in OLT (if no man-in-the-middle threat)**
- Privacy
  - The knowledge of neighbors MAC addresses, or the amount and type of traffic can be seen as a privacy violation
  - Downstream MPCP messages can reveal upstream traffic characteristics of each ONU

  ⇒ **MAC addresses and MPCP messages should be encrypted**

Overview of security mechanisms for EPON

Mechanism	Standard
Authentication	802.1x
Access control	802.1x
Key exchange	802.1x
Re-keying	802.1x
Key transfer to cipher	802.3ah
Key change indication	802.3ah
En/decryption indications	802.3ah
Cipher counter synchronization	802.3ah
Encryption key derivation ?	802.11i ?
Cipher	802.11i ?

Encryption functions

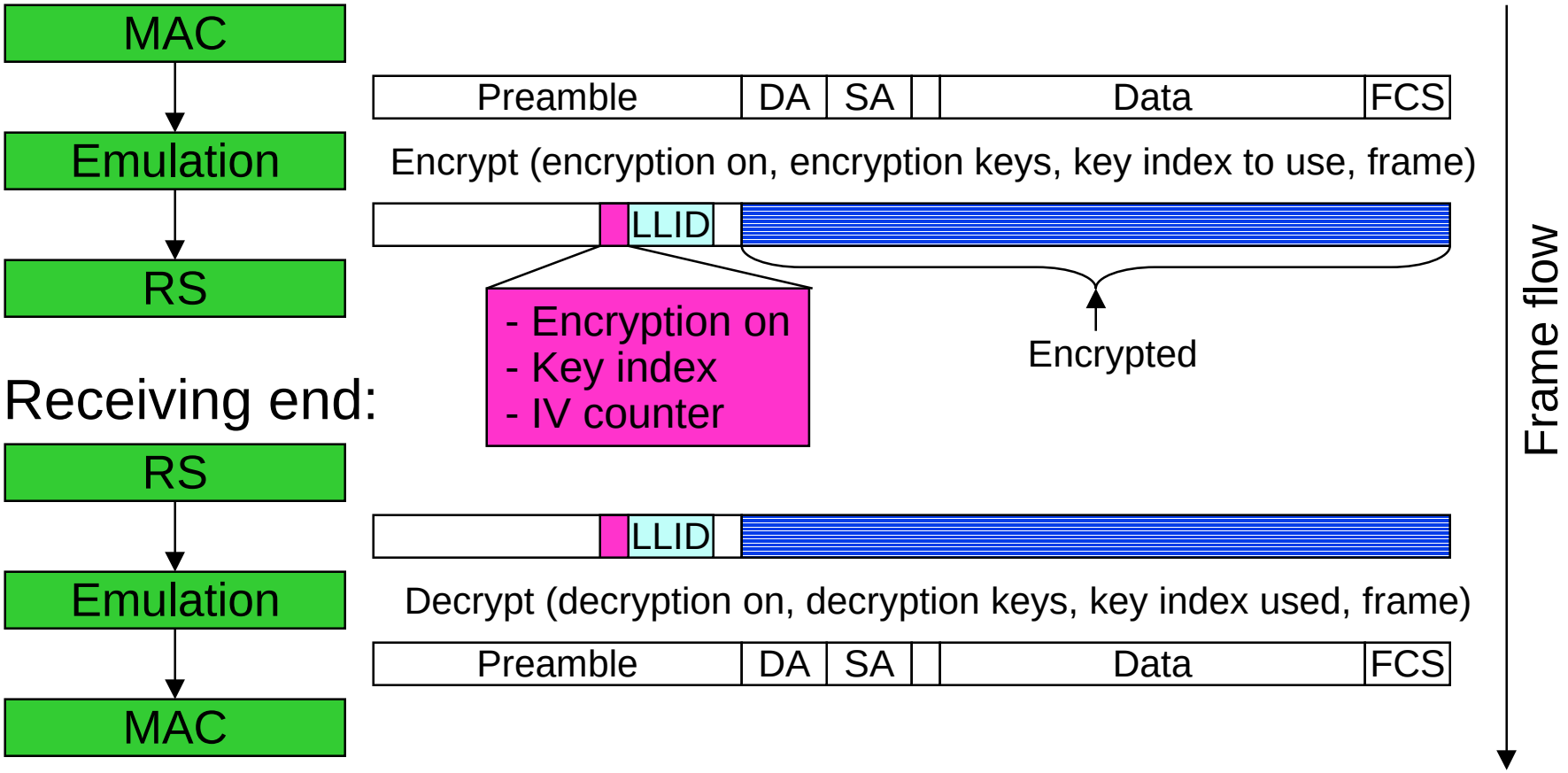
- Encryption is on the Emulation Layer below MAC
  - This allows encryption of MAC addresses, OAM frames and MPCP messages
- Emulation Layer have optional Encrypt and Decrypt functions for each ONU separately
  - Encrypt (encryption on, encryption keys, key index to use, frame)
  - Decrypt (decryption on, decryption keys, key index used, frame)
- Parameter values are read/written from/to registers
  - Encryption on (read) - Enables/disables encryption frame by frame
  - Decryption on (write) - Indication to upper layer that frame was decrypted
  - Encryption/decryption keys (read) - Keys transfer to cipher
  - Key index to use (read) - Indicates which encryption key to use
  - Key index used (write) - Indicates which decryption key was used
- Frames passes always through the function if it is implemented

Frame content

- Full MAC frame (from DA to FCS) should be encrypted
  - Privacy requires encryption of DA and SA
  - Confidentiality requires encryption of payload
  - Privacy and confidentiality requires encryption of FCS
  - Correctly decrypted CRC is used as message authentication (see separate presentation)
- Encryption requires three fields from the preamble
  - Encryption on [1 bit] flag indicates whether the frame is encrypted or not
  - Key index [1 bit] indicates which key to use in the decryption. This is needed for smooth key change (see separate presentation)
  - IV counter [2 bits] keeps initialization vectors (IV) at transmitting and receiving ends synchronized. This is needed by ciphers (see separate presentation)

Frame flow

- Transmitting end:



- Receiving end:

Properties of Encryption

- Emulation Layer have optional Encrypt and Decrypt functions for each ONU separately
- Encryption can be enabled/disabled frame by frame
- Full MAC frame (DA - FCS) is encrypted
- Message authentication is possible by checking correctness of the decrypted CRC
- Encryption maintains packet length
- Encryption functions should have unchanging delay regardless of the parameter values
  - Varying delay would affect to RTT and thus cause collisions
- Mechanism includes means to be able to use other standards
  - Encryption_on flag to enable/disable encryption
  - Key change indication for key exchange
  - IV counter for synchronizing initialization vectors