CTR Mode for Encryption

Onn Haran – Passave

Olli-Pekka Hiironen – Nokia

Disclaimer

- This presentation is informative
- The described functionality should not be part of 802.3

How Cipher Block is Applied?

- When using a symmetric block code (like AES), the plaintext is divided into blocks (128-bit in AES case)
- The mathematical operations, in addition to encryption function, are called Block Cipher Mode of Operation
- Some modes of operation requires an Initialization Vector (IV), which is used in the initial step of encryption/decryption

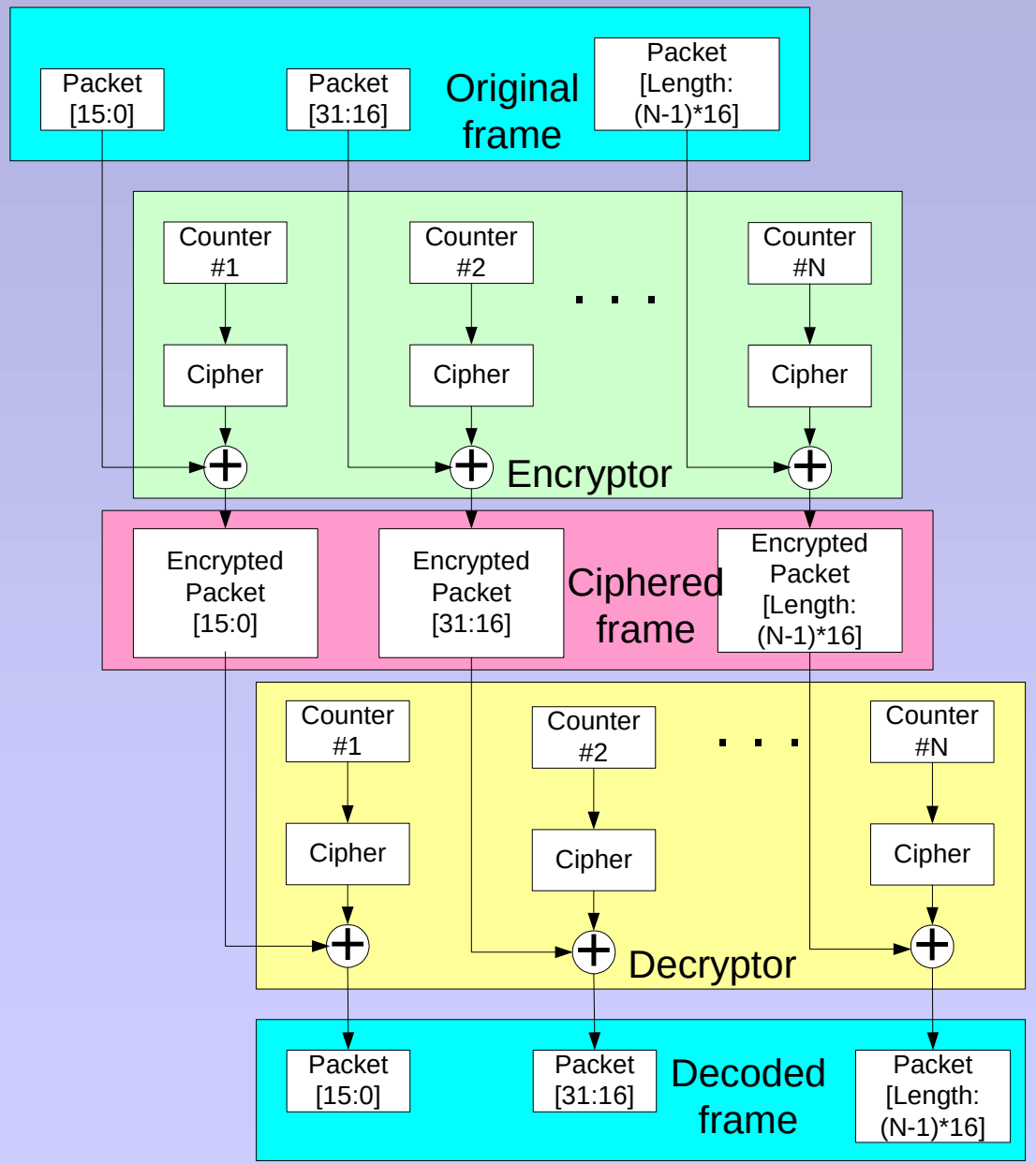
Why Block Cipher Mode of Operation is Needed?

- **Advantages of adding Block Cipher Mode of Operation are:**
  - The same plaintext will be encrypted to a different ciphertext, at any invocation
    - Important when analyzing repeating patterns (DA, SA, Ethertype, IP headers, TCP headers, known packets like ICMP, ARP, etc…)
  - Helps in handling last block problem
    - Last block can be smaller than code block size
  - Impossible to perform packet replay
  - Increases encryption level

Block Cipher Mode of Operation Recommendation

- **National Institute of Standards and Technology (NIST) recommends 5 block cipher modes of operation (publication 800-38A)**
- **Two features are required:**
  - Maintaining packet length – Length of last block should be arbitrary
  - Enabling parallel encryption - Encryption of a plaintext block shouldn’t depend on result from previous block
- **From these modes only Counter (CTR) mode supports both features**
- **Additional mode Offset Codebook (OCB) was proposed for 802.11, but it is protected by patents**

Frame Format – CTR mode



Counter Initialization Vector (IV)

- **Counter Initialization Vector must be used only once (nonce) per a specific key**
- **The counter is based on PON clock**
- **The counter IV will be a concatenation of:**
  - cycle_counter [32 bits]
  - (PON clock+ 16)[32:5] – PON clock rounded to the closest 512nSec boundaries
  - N [7 bits] – Serial number of cipher block inside frame

Counter Initialization Vector (IV)

- **32-bit cycle_counter is incremented whenever PON clock wraps around**
  - LSB of cycle_counter is transmitted in preamble
  - ONU resets cycle_counter when changing keys
  - OLT monitors changes in key number. When detected:
    - Counter is reset if LSB is 0
    - Counter is set to 32'h0000_0001 if LSB is 1