Scrambling in 10G Ethernet and applicability to 10G EPON

Jeff Mandin

802.3av Task Force – Dallas

Nov 2006

Agenda

PMC-SIERRA

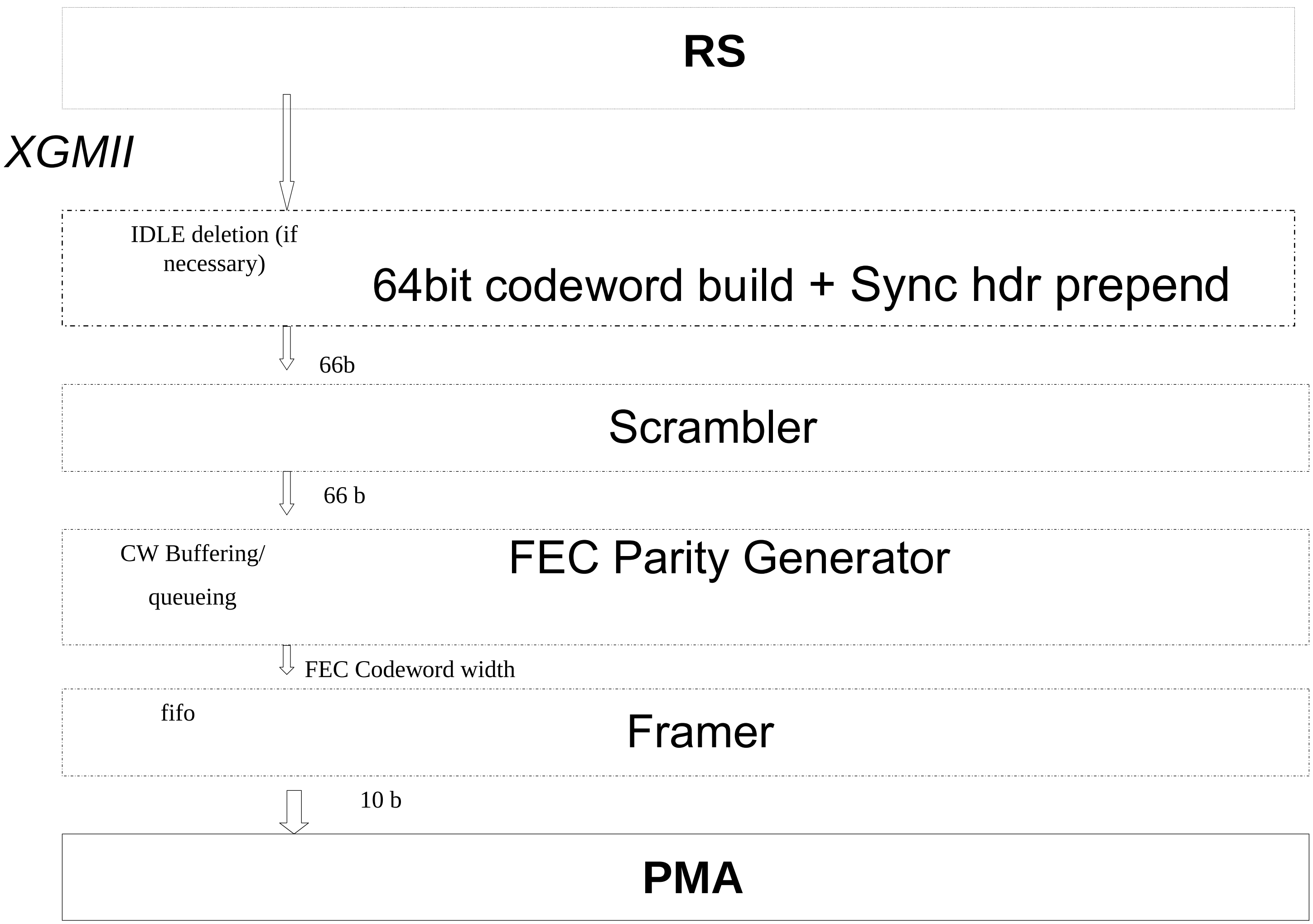
1. Position and behaviour of scrambler function

2. Scramblers in 10G ethernet
   a) Pseudo-random Bit Stream (PRBS)
   b) Self-synchronous scrambler
   c) Interlaken scheme

3. Considerations for 10G EPON scrambler

4. Conclusions

Position of scrambler in the 10GEPON PCS layer



Scrambler Function

PMC-SIERRA

- Bit stream to the PMA should be DC-balanced and have a limited maximum run length in the same fashion as random data
  - Different balance characteristics than 8/10 line code
- Scrambling is applied at the transmitter to 66b codewords before FEC
- The transmitter does not scramble the parity bytes before sending over PMA (parity byte sequence is expected to be DC balanced).
- At the receiver FEC will detect and repair errors in the scrambled codewords before the descrambling is applied

Types of Scrambling: Pseudorandom Bit Sequence (PRBS)

- PRBS-based scrambler uses Linear Feedback Shift Register with a particular initial state to generate a cyclical sequence of pseudo-random bits

- The transmitter performs scrambling by XOR-ing the data with the pseudo-random output

- Issues:
  - Requires set/reset synchronization
  - Vulnerable to “killer packet” attack

Types of Scrambling: Self-synchronous scrambler

- Modification to the PRBS scheme: the transmitted/received data is itself used as the input to the LFSR state.
- No need for set/reset synchronization
  - Instead: initial bits (eg. First 43 bits) of transmission will be lost while the receiver's descrambler acquires its initial state
- Killer packet resistance
  - Attacker will typically not know the state of the scrambler so as to be able to generate a pattern that would disrupt the receiver
- Issues:
  - Data loss during synchronization
  - Error multiplication
    - 1 bit error in scrambled data becomes 2 bit errors in unscrambled data

Types of Scrambling: Interlaken scheme

PMC-SIERRA

- Interlaken is a chip-to-chip protocol based on SPI 4.2
- Uses PRBS mechanism
- Attains killer packet resistance and better DC balance by dynamically inverting 66b words to maintain a low running disparity
    - Claims to better avoid “baseline wander”
- Requires an extra bit of overhead (“64/67 coding”)

Considerations for 10GEPON downstream

PMC-SIERRA

- Synchronization:
  - Can do set/reset synchronization based on FEC block boundaries
  - Can also do self-sync (initial data loss not a problem)
- Killer packets unlikely to be a concern
  - Attacker would need to control alignment of data into 66b codewords and FEC blocks at OLT

➤ Downstream can probably use any of the above mechanisms

Considerations for 10GEPON upstream

PMC
PMC-SIERRA

Burst mode creates special requirements:

- Fast synchronization
  - Self-synchronous scrambler delay/data loss is problematic
- Killer packets are a concern
  - Can appear as first frame in upstream burst

Conclusion

- Need to select or create 10GEPON scrambler definition based on the requirements posed by upstream burst mode