Efficient Security Encapsulation for IEEE 802.16m

Document Number:

IEEE S802.16m-09/0995

Date Submitted:

2009-04-27

Source:

David Johnston
Avishay Shraga
Xiangying Yang
Intel Corporation E-mail: avishay.shraga@intel.com

Re:

IEEE 802.16m-09/0020, “Call for Contributions on Project 802.16m Amendment Working Document (AWD) Content”.
Category: AWD - New Contribution / Area: Chapter 15.2.3 (Security)

Base Contribution:

Re: C802.16m-09/0995

Purpose:

To improve the cryptographic signaling overhead in MAC PDUs.

Notice:

This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups. It represents only the views of the participants listed in the “Source(s)” field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.

Release:

Patent Policy:

Security Format

- Requires addition of PN & ICV over protected data.
- Several Options
  - Multiplexed protected PDU (E.G. See 1509r1)
  - Per PDU protection (16e.)
  - Per SDU protection
  - Per Burst Protection
- Must cover management PDU protection
- Must cover signaling PDU protection
- Should be efficient

Security Format Efficiency Issues

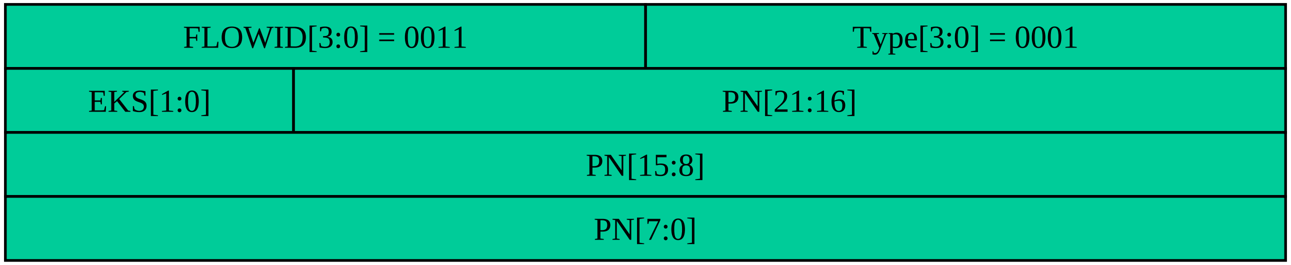
- Per PDU (16e)
  - Good for packed SDUs
  - Bad for fragmented SDUs
- Per SDU
  - Good for fragmented SDU
  - Bad for packed SDUs
  - Fails to protect MAC level signaling (headers & subheaders) aren’t SDUs)
- Per burst
  - Good for big bursts
  - Bad for small bursts (e.g. at cell edge, where allocations are small)
- We want a method that can adapt itself to these different scenarios and can protect management and signals

Adaptive Security Format

- Goal
  - to allow both per-PDU or per-SDU encryption, as needed, while still allowing management and signaling headers to be protected
- Separate PN and ICV from PDU format
  - Define PN signaling PDU and ICV signaling PDU.
    - These can be inserted in the PDU stream like any other header
    - Data between PN and ICV headers is protected
    - Signals are fixed size. Keeping overhead low – no length field.
  - Allow transmitter to insert them wherever it is appropriate, even across burst boundaries.
    - Efficient for both packed and fragmented traffic.

PN & ICV Signaling Headers

- PN Signaling Header



FLOWID[3:0] = 0011 | Type[3:0] = 0001

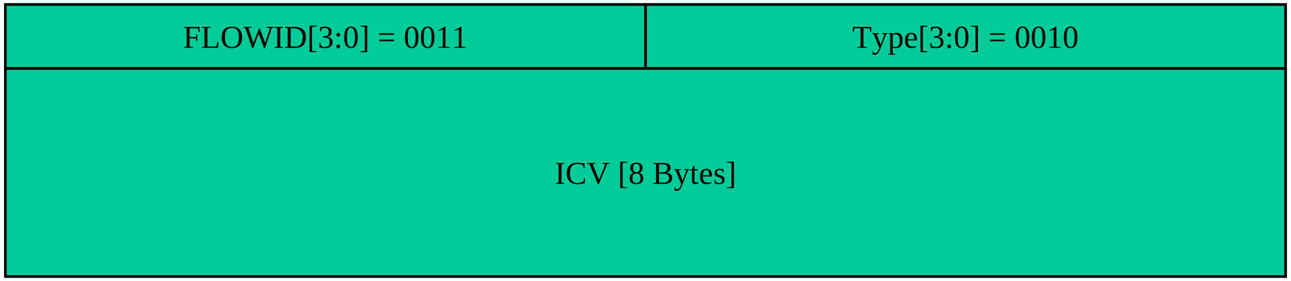
EKS[1:0] | PN[21:16]

PN[15:8]

PN[7:0]

4 bytes

- ICV Signaling Header

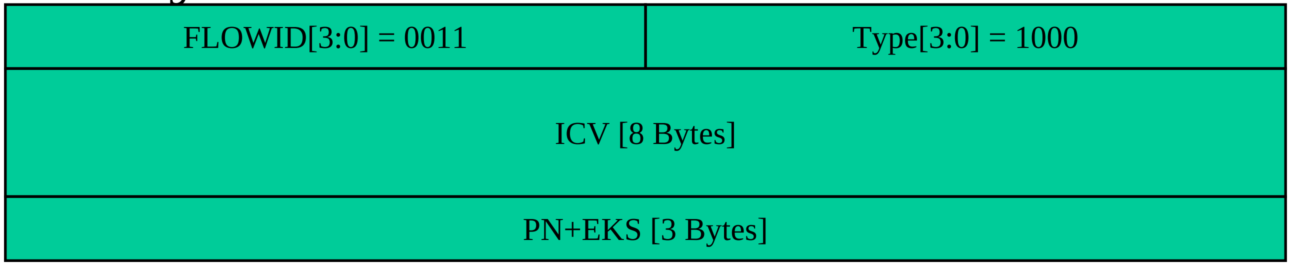


FLOWID[3:0] = 0011 | Type[3:0] = 0010

ICV [8 Bytes]

9 bytes

- Possibly - Combined for back to back ICV+PN



FLOWID[3:0] = 0011 | Type[3:0] = 1000

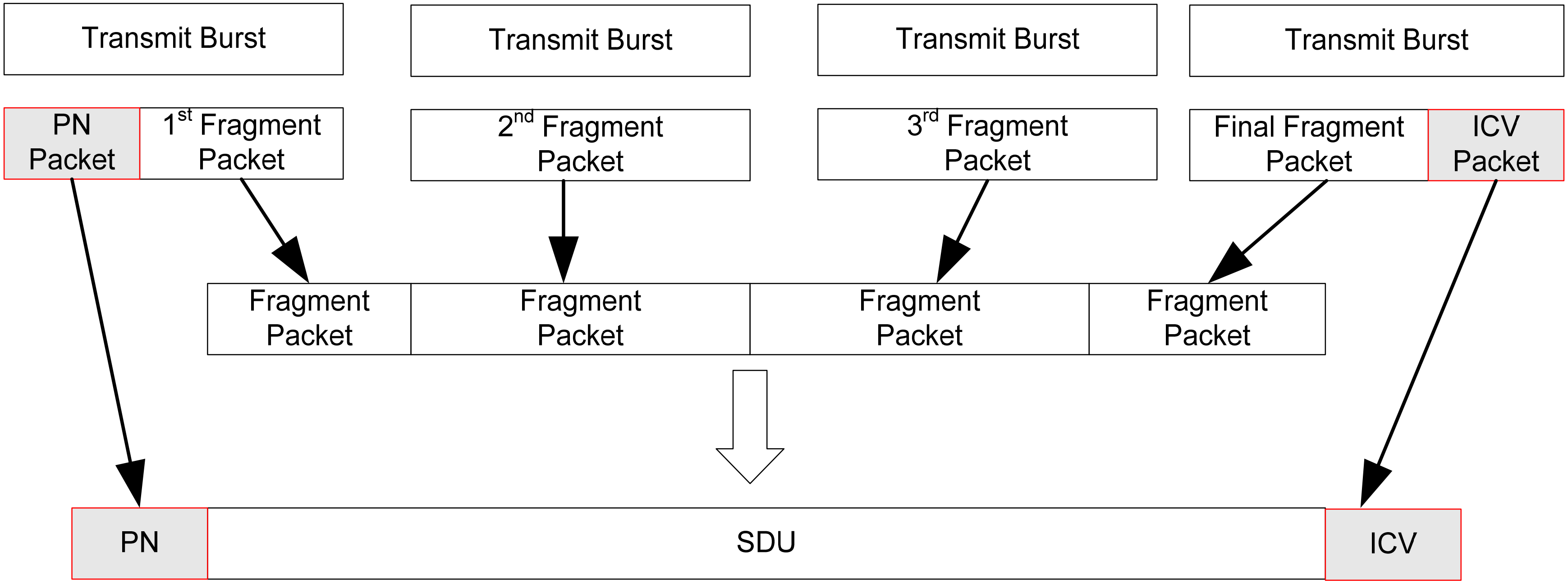
ICV [8 Bytes]

PN+EKS [3 Bytes]

12 bytes

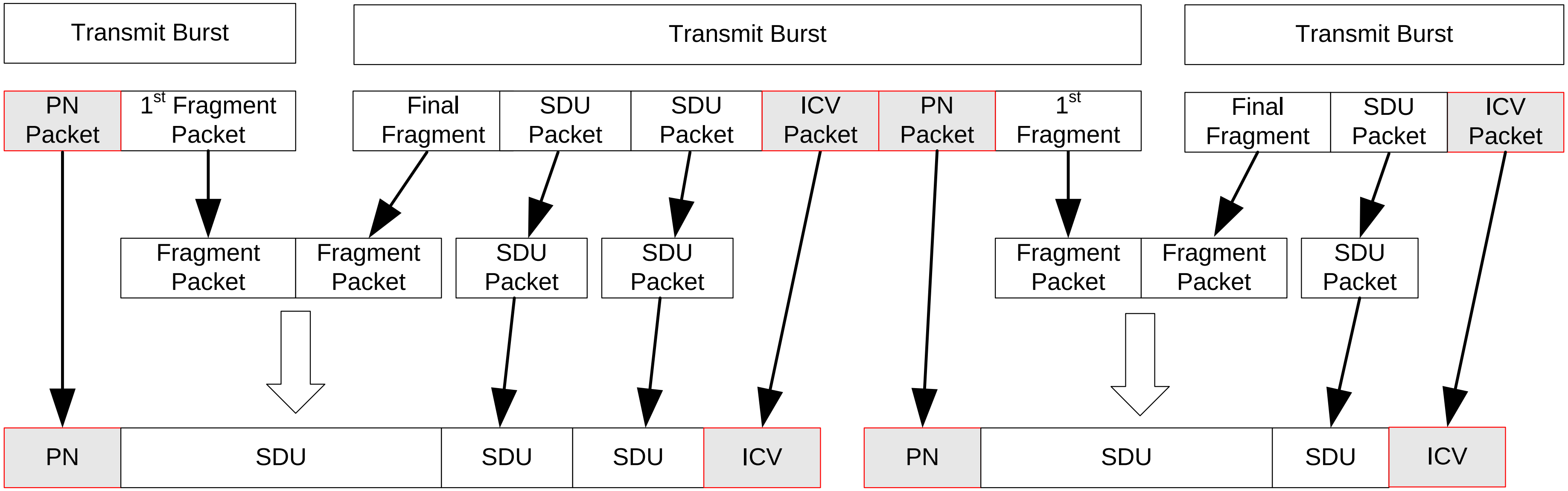
Adaptive Security Format

- Efficient for Fragmented packets.
  - Works well with cell edge scenarios.



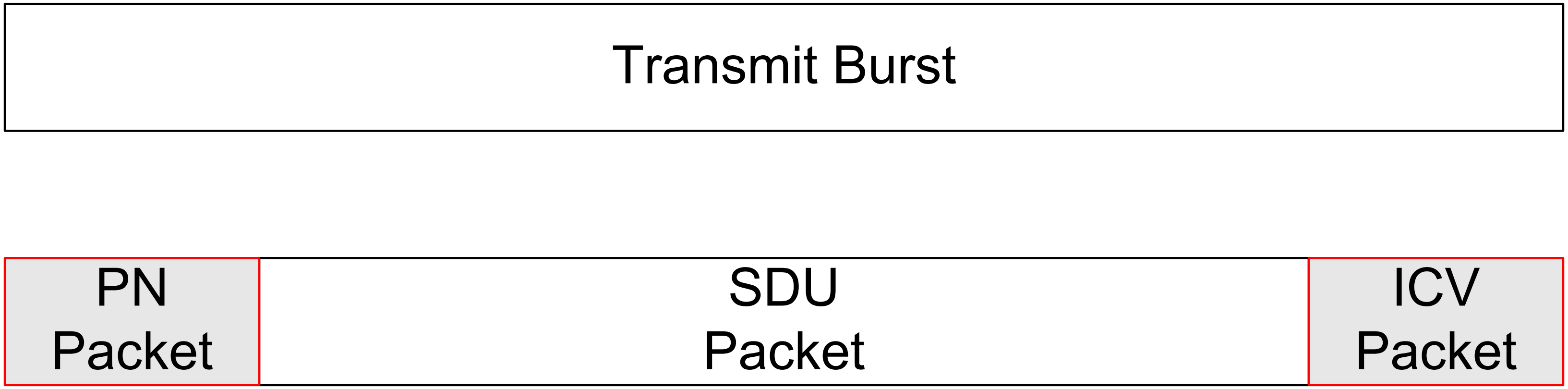
Adaptive Security Format

- Heavy data scenarios.
  - Works well with cell edge scenarios.
  - Transmitter would insert PN&ICV before initial 1st fragment at end of burst.



Adaptive Security Format

- Single PDU



Transmit Burst

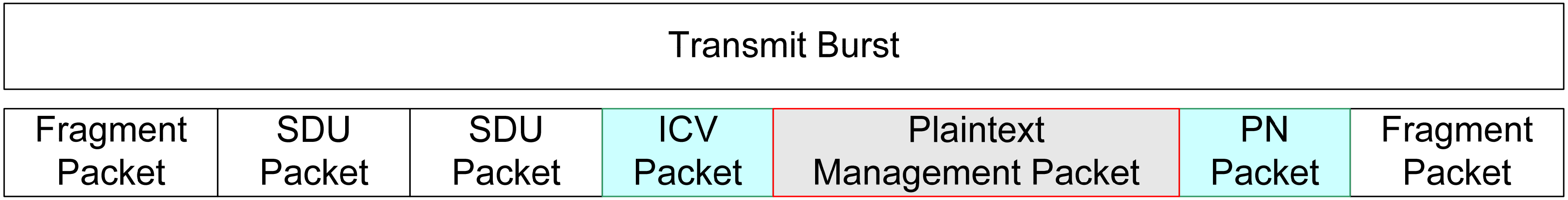
PN Packet

SDU Packet

ICV Packet

Incorporating plaintext PDUs

- Need to be able to send plaintext management PDUs
  - Insert them between protected fields.
  - I.E. One or more plaintext management PDUs can follow any ICV packet



Transmit Burst

Fragment Packet | SDU Packet | SDU Packet | ICV Packet | Plaintext Management Packet | PN Packet | Fragment Packet

Example Efficiency Calculation using 16e numbers

- In the worst case, for standalone packets, the efficiency would be the same as for the existing protocol. 1 PN + 1 ICV per PDU.
- For large packets in poor signal conditions: In 16e, for a 1500 byte IP packet in a cell edge with 48 bytes of data per 60 byte transmit allocation, there would be 32 fragments, each with 12 bytes of overhead per fragment. Giving 384 bytes of overhead for 1500 bytes of data = **25.6% overhead**.
- In this proposal there would be 26 fragments. The first with a PN and the last with an ICV. The overhead would be 12 bytes per 1500 bytes of data = **0.8% overhead**.

Complexities

- When you encrypt a block of data, you must know the size in order to construct the nonce.
  - In 16e, CCM encryptor/decryptor can infer length from GMH
  - In 16m encrypted field size must be elsewhere to describe length of multiple PDUs over which CCM operates. E.G. in PN header.
  - But you don’t necessarily know the size of subsequent bursts in fragmented traffic and you don’t necessarily know what subheaders, headers or management PDUs will be inserted between fragments. So either:
    - Pad the DLEN field in and declare in PN – increases the tag size.
    - Or Use a online mode. E.G. GCM – as used in 802.3 (with 802.1ae)
- HARQ may reorder bursts, breaking decryption
  - Reordering of bursts is needed
  - Must have HARQ reordering SN in map, PN header or elsewhere.

AWD text proposal

- High level view
  - Encryption encapsulation format
    - Scope of encryption encapsulation (across single or multiple bursts/PDUs)
    - PN Signaling Header
    - ICV Signaling Header
    - GCM Mode
    - Document overhead against important scenarios
      - Across multiple fragments
      - Across a packed burst
      - Across a single PDU
      - Indicate support for SRTP for VoIP in place of L2 security encapsulation.

- Adopt the text proposal in C802.16m-09/0995