802.16 CID Number Space Management

IEEE 802.16 Presentation Submission

Document Number:

IEEE C802.16d-03/65

Date Submitted:

2003-09-10

Source:

David Johnston	Voice:	503 264 3855
Intel	Fax:	503 202 5047
2111 NE 25th	E-mail:	dj.johnston@intel.com, david.johnston@ieee.org
Hillsboro, OR 97124		

Venue:

September 2003 802.16 Interim, Denver, CO

Base Document:

Purpose:

Description of proposed amendments to enable efficient key retrieval implementations.

Notice:

This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Release:

The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.

IEEE 802.16 Patent Policy:

The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

CID Number Space Management

David Johnston, Intel,
dj.johnston@intel.com

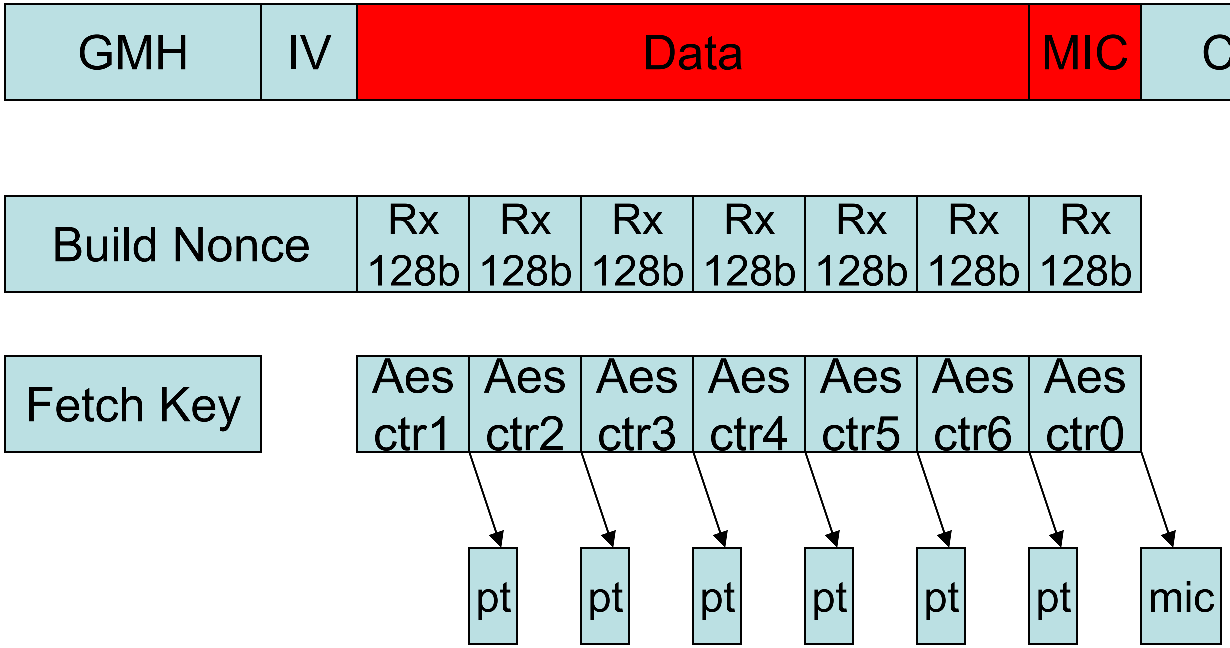
CIDs/Key mapping

- The CID determines the TEK
  - When a packet is received the receiver retrieves the key associated with that CID
  - The CID number space is 65536 entries long
    - A 65536 entry key table is not reasonable
    - So an implementation must use a search mechanism to find the key entry associate with a CID. The CID cannot be used directly as an index
      - CAM, hash function, binary chop, linear search etc
- It takes either time or lots of storage to get keys. You can’t save on both.

The problem with Key Retrieval Time

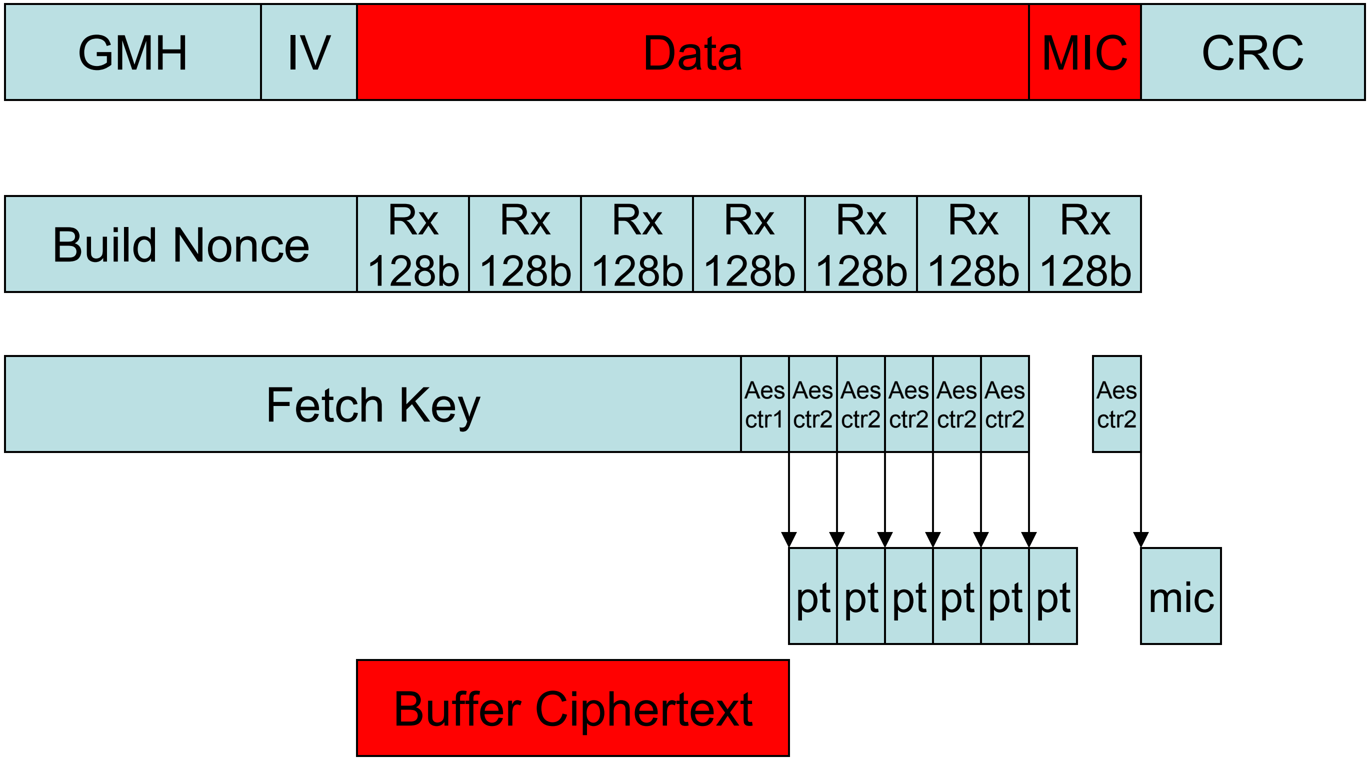
- In early decrypt models, popular with stream cipher modes (like CCM), the key is fetched as soon as the CID arrives and this is used to generate a stream cipher to decrypt the incoming packet.
- The longer the key retrieval latency, the larger the elasticity (buffering) required at the front of the MAC

Key Available Early



- Cipher stream generated ahead of data
  - Plain text available as soon as data arrived + 1 XOR gate
  - AES latency = 11 clocks.
  - Buffering requirement less than internal buffer in AES block
    - No additional buffering requirement

Key Available Late



- Cipher stream generated after data arrival
  - Data must be buffered
  - Plaintext can be delayed through MAC on short packets

A Solution

- SS Indicates max number of supported SAs == max number of key entries in key table
- BS gives SS an offset into the CID space
  - BS partitions CID space between SSs
  - All assigned secure CIDs go in that space
- SS calculates (CID-offset) on receipt of packet
  - Can use this to index directly into key table
  - Single memory lookup!

Benefits

- No complex key retrieval hardware
  - Hashing, binary chopping, scanning
- Deterministic key retrieval time
- Short key retrieval time
- Guaranteed no buffering at front of MAC

Where to Apply

- Enhanced security requires more per CID state
  - 2 * 128 bit keys
  - Rx PN
  - Tx PN
- CID space management should be mandated along when enhanced security is implemented