Compression of IPsec AH and ESP Headers for Constrained Environments

draft-raza-6lo-ipsec-04

{shahid.raza, simon.duquennoy}@sics.se
goran.selandaer@ericsson.com

Status of the Document

- First submitted as a position paper to the Smart Object Workshop [RFC6574] co-located with IETF 80.
- Later submitted to 6LoWPAN WG
- Moved to 6lo and included in the 6lo BoF
- Presented in 6lo during the IETF93
- Presented in 6lo during the IETF94

Salient Features

- Does not require any modification in the IPsec standard
  - End-to-End compatible with any IPsec enabled hosted on the Internet.
  - Only performs header compression within 6LoWPAN networks without compromising any security properties
- Seamlessly links with the 6LoWPAN standard
- Other compression mechanisms exists
  - draft-mglt-6lo-diet-esp-01 requires changes in the IPsec standard and should also be supported/enabled in hosts on the Internet
  - ROHC [RFC5795][RFC5856]) also targets any Internet hosts and not specific to 6LoWPAN networks
  - Both are complementary to our solution

IETF94 Comments

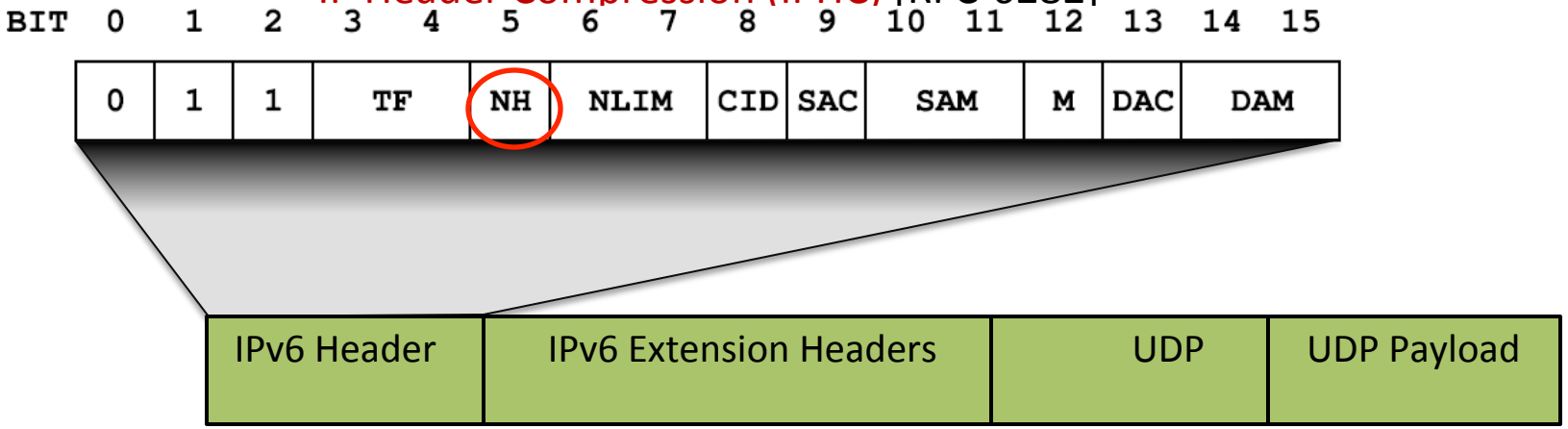
- AH is almost not used today; why should we include it in this draft?
  - A paragraph is added in the introduction section on the use of AH in the IoT.
- Why the proposed ESP NHC ID-bits are taken from the IANA's assigned bit?
  - One of the free ID-bits are now used.
- Use only one EID reserve bit and make the other bit extensible.
  - Done
- Why not to use CCM?
  - This draft does not recommend or mandates any specific cipher suites; it only compresses the headers.

IP Security (IPsec)

- End-to-end Security at the Network layer
  - Part of the OS
  - Protects IP and UDP/TCP headers
  - IPsec Transport mode for the Internet of Things
- Authentication Header (AH) [RFC-4302]
  - Integrity and authentication
- Encapsulated Security Payload (ESP) [RFC-4303]
  - Confidentiality and optionally integrity and authentication
- AH and ESP are *IP extension headers*
- IPv6 nodes SHOULD implement IPsec [RFC 6434]

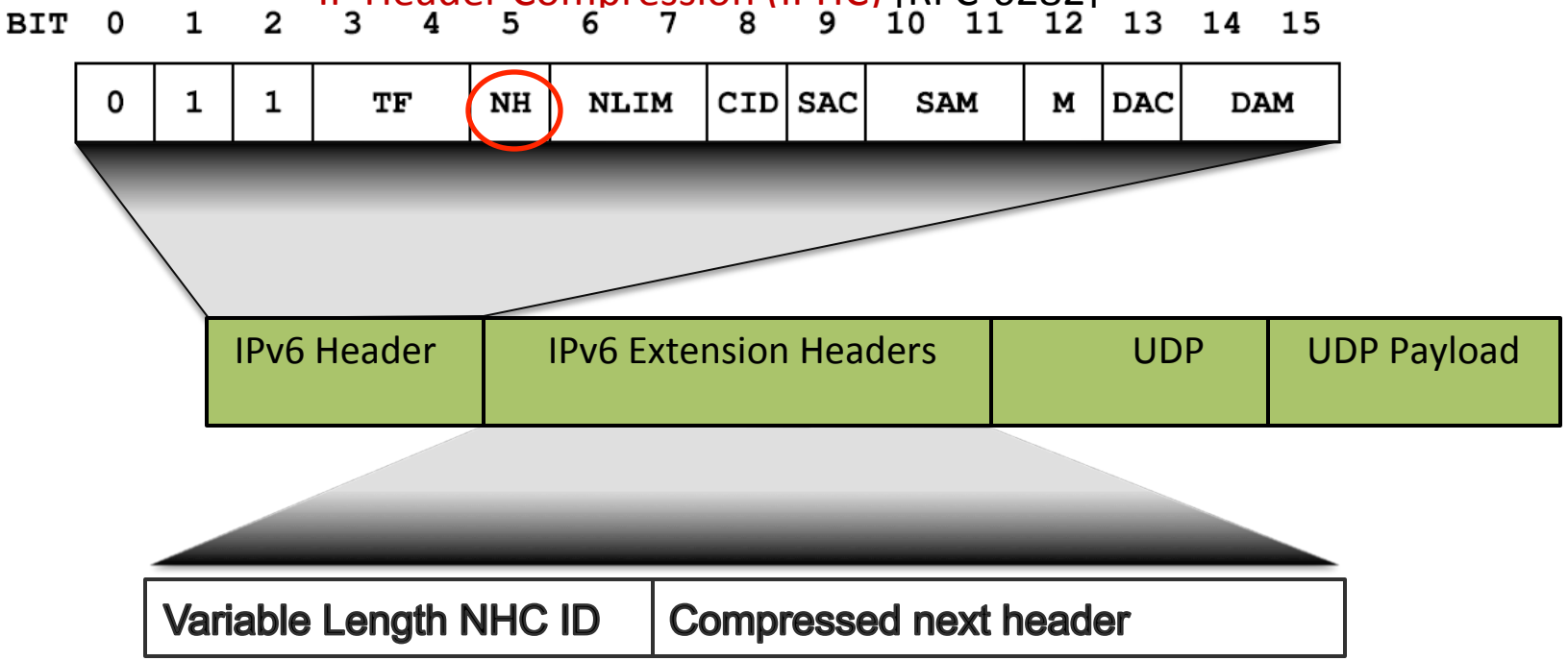
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]



Linking IPsec Headers Compression with 6LoWPAN

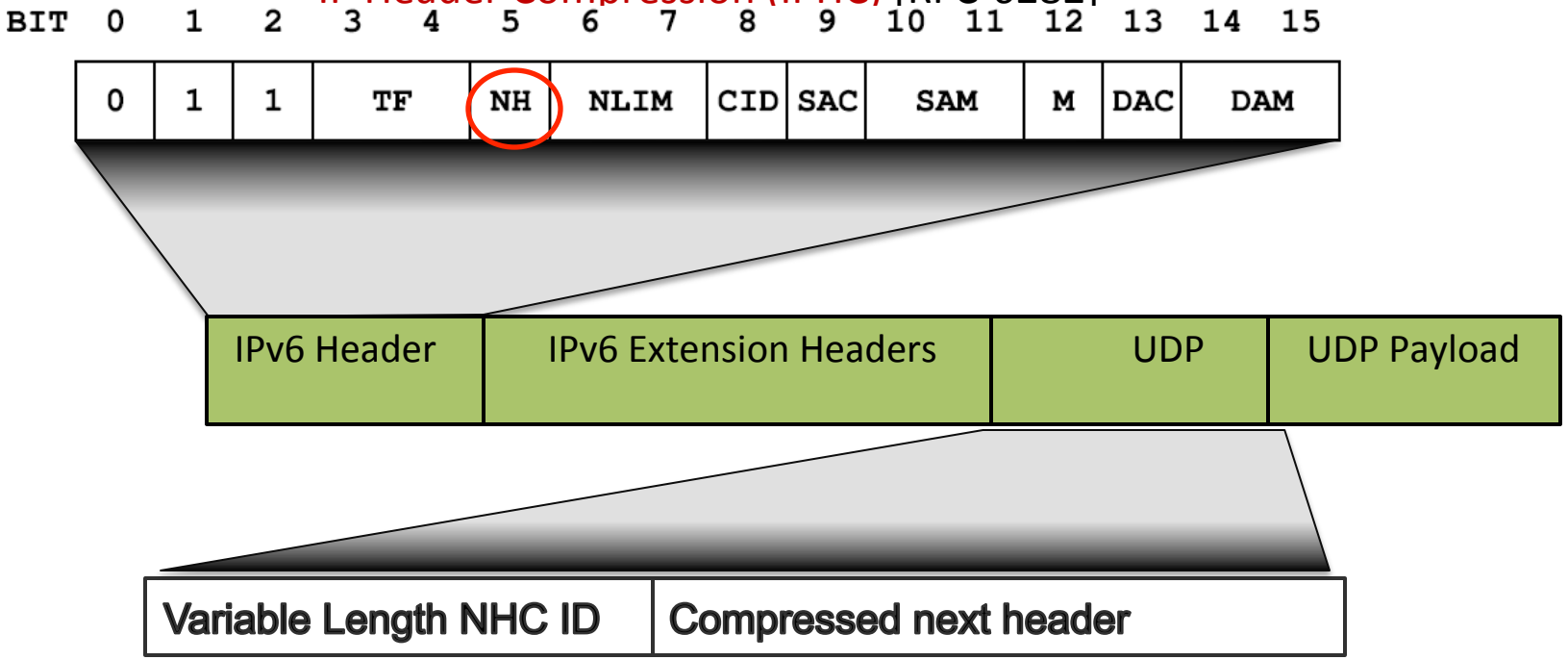
IP Header Compression (IPHC) [RFC-6282]



Next Header Compression (NHC) [RFC-6282]

Linking IPsec Headers Compression with 6LoWPAN

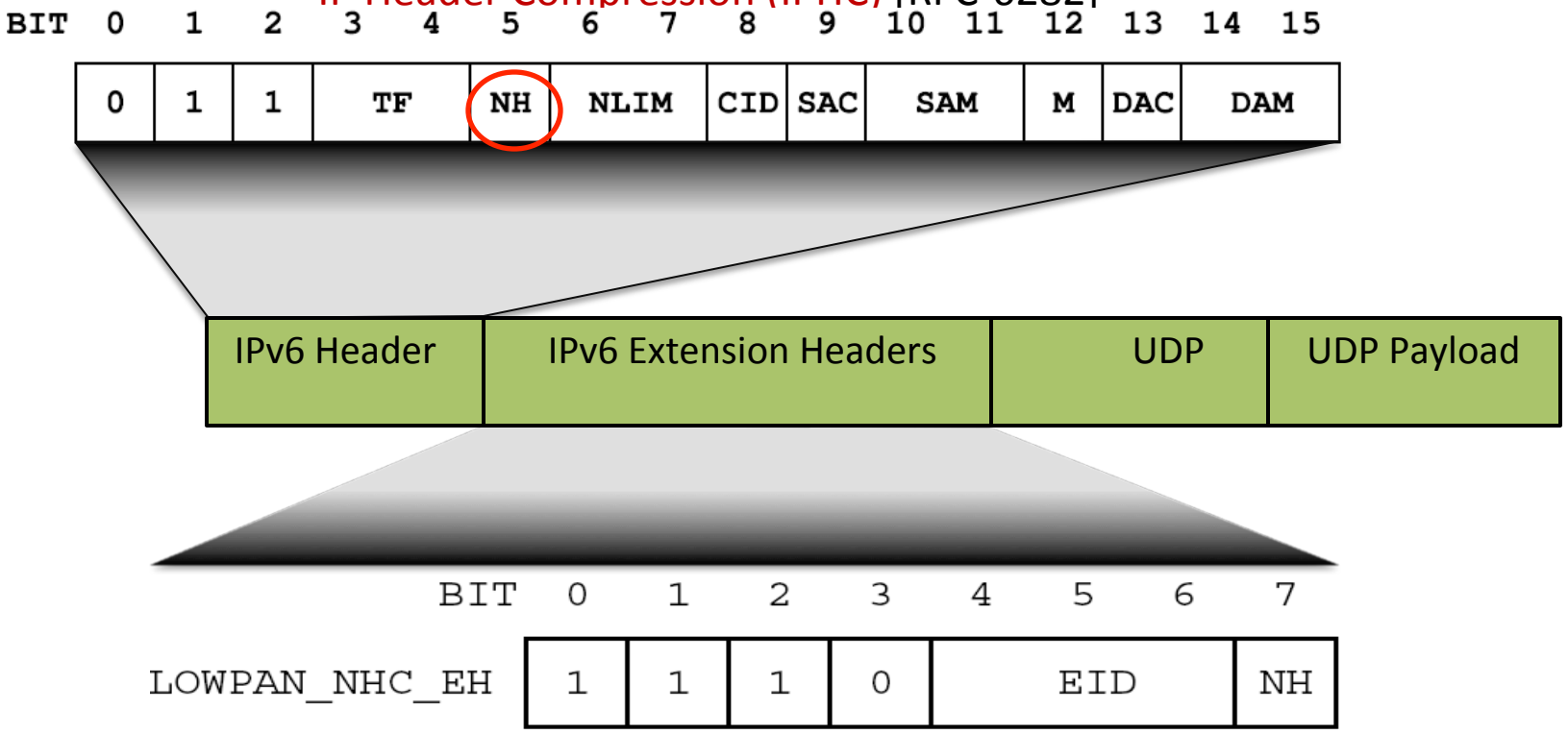
IP Header Compression (IPHC) [RFC-6282]



Next Header Compression (NHC) [RFC-6282]

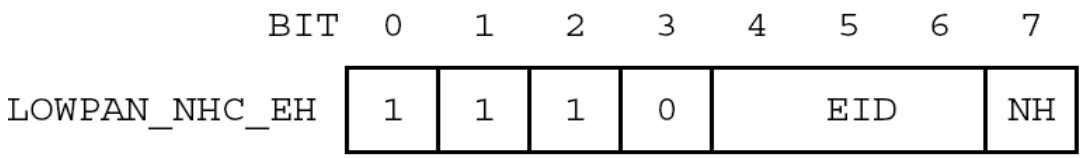
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]



Next Header Compression (NHC) [RFC-6282]

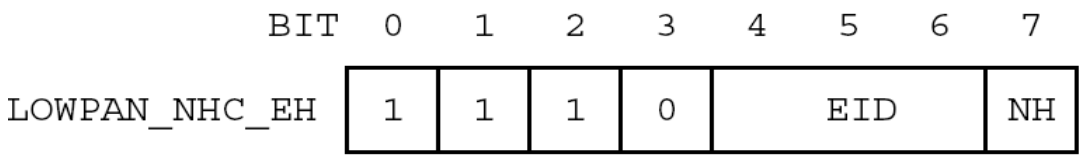
Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header

Linking IPsec Headers Compression with 6LoWPAN (cont…)

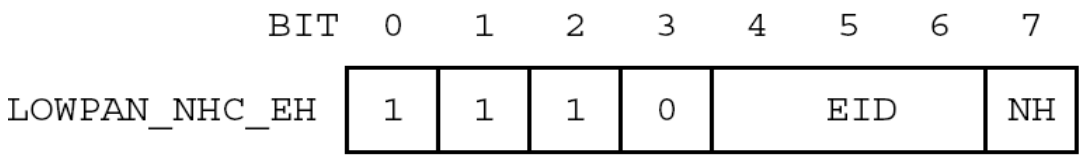


Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header

Extension Header Order [RFC2460]
IPv6 header
Hop-by-Hop Options header
Destination Options header
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header
upper-layer header

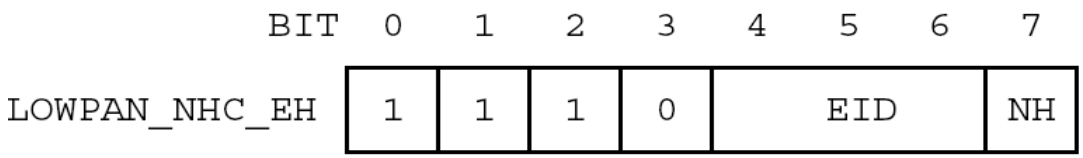
Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved - IPv6 Authentication Header
6: Reserved -IPv6 Encapsulated Security Payload
7: IPv6 Header

Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

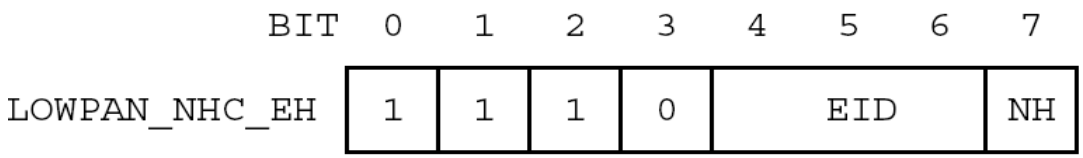
0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved - IPv6 Authentication Header
6: Reserved -IPv6 Encapsulated Security Payload
7: IPv6 Header

Proposal 2 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved
6: *Reserved IPv6 Authentication Header & IPv6 Encapsulated Security Payload
7: IPv6 Header

**** Variable length NHC ID is used to distinguish AH and ESP***

Linking IPsec Headers Compression with 6LoWPAN (cont…)



Proposal 1 - IPv6 EID:

0: IPv6 H… Hop Options …
1: IPv6 R… eader
2: IPv6 Frag… ade…
3: IPv6 Destina… eader
4: IPv6 Mobility H…
5: Reserved - I… ation Header
6: Reserved … Security Payload
7: IPv6 He…

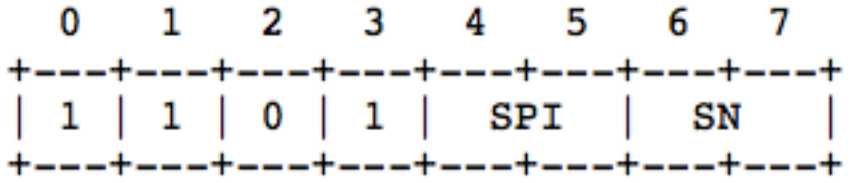
Proposal 2 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved
6: *Reserved IPv6 Authentication Header & IPv6 Encapsulated Security Payload
7: IPv6 Header

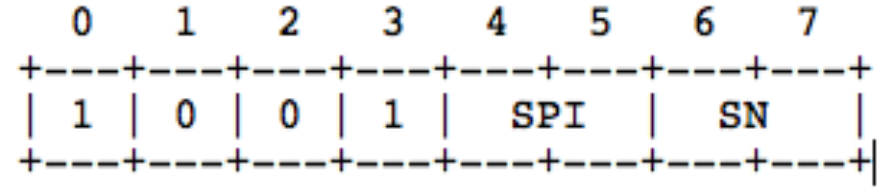
**** Variable length NHC ID is used to distinguish AH and ESP***

Compressing IPsec (cont...)

- Proposed LOWPAN NHC encoding for AH



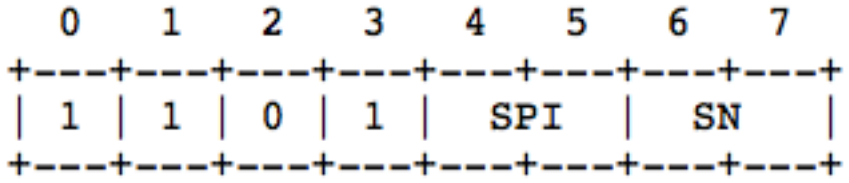
- Proposed LOWPAN NHC encoding for ESP



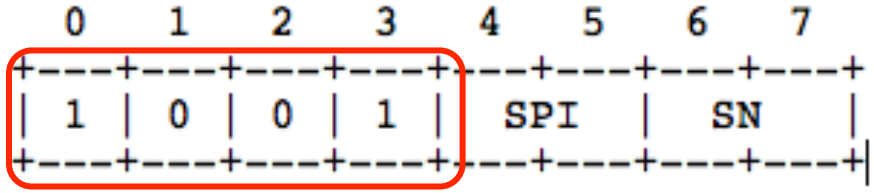
- SPI: Security Parameter Index
- SN: Sequence Number

Compressing IPsec (cont...)

- Proposed LOWPAN NHC encoding for AH

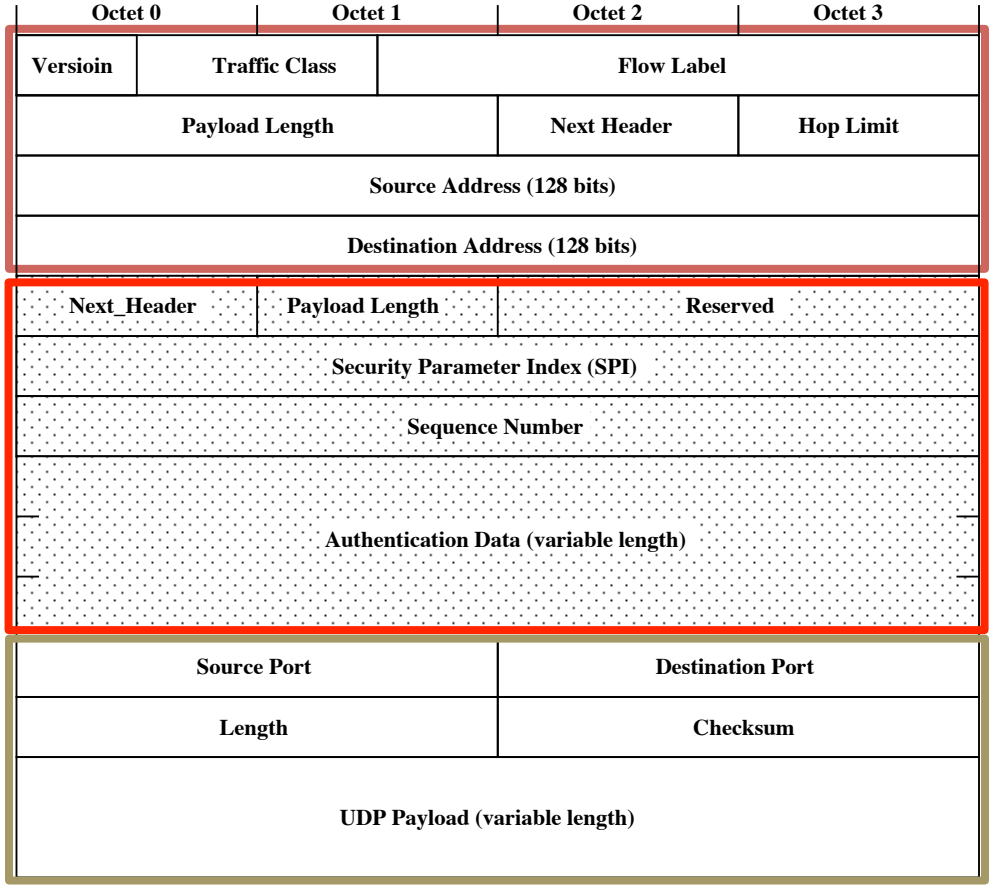


- Proposed LOWPAN NHC encoding for ESP

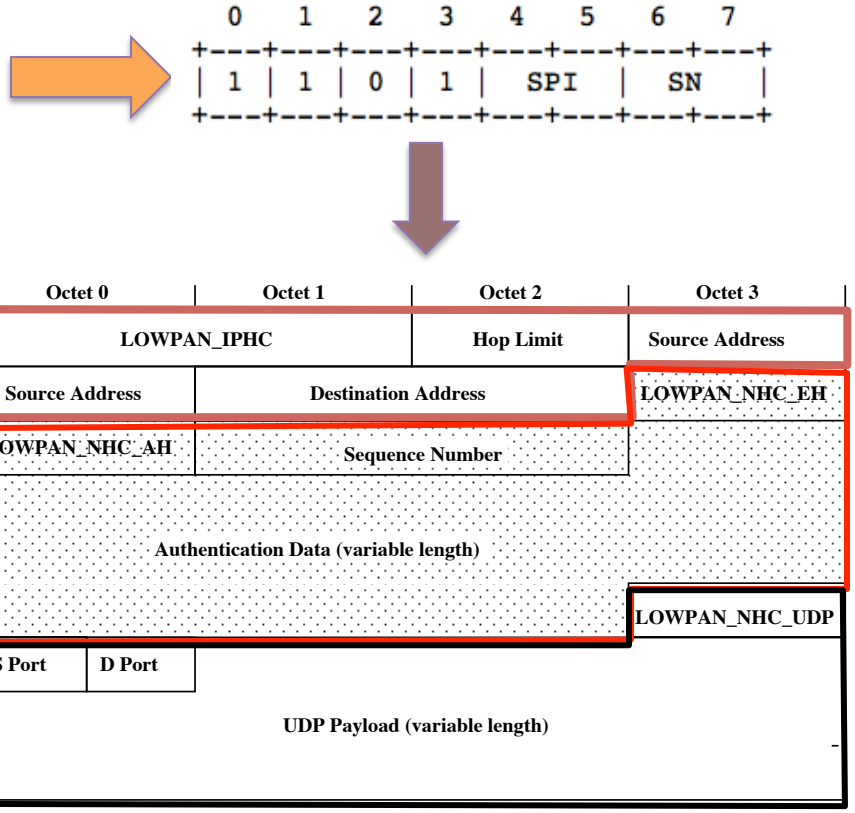


- SPI: Security Parameter Index
- SN: Sequence Number

Compressed IPsec AH



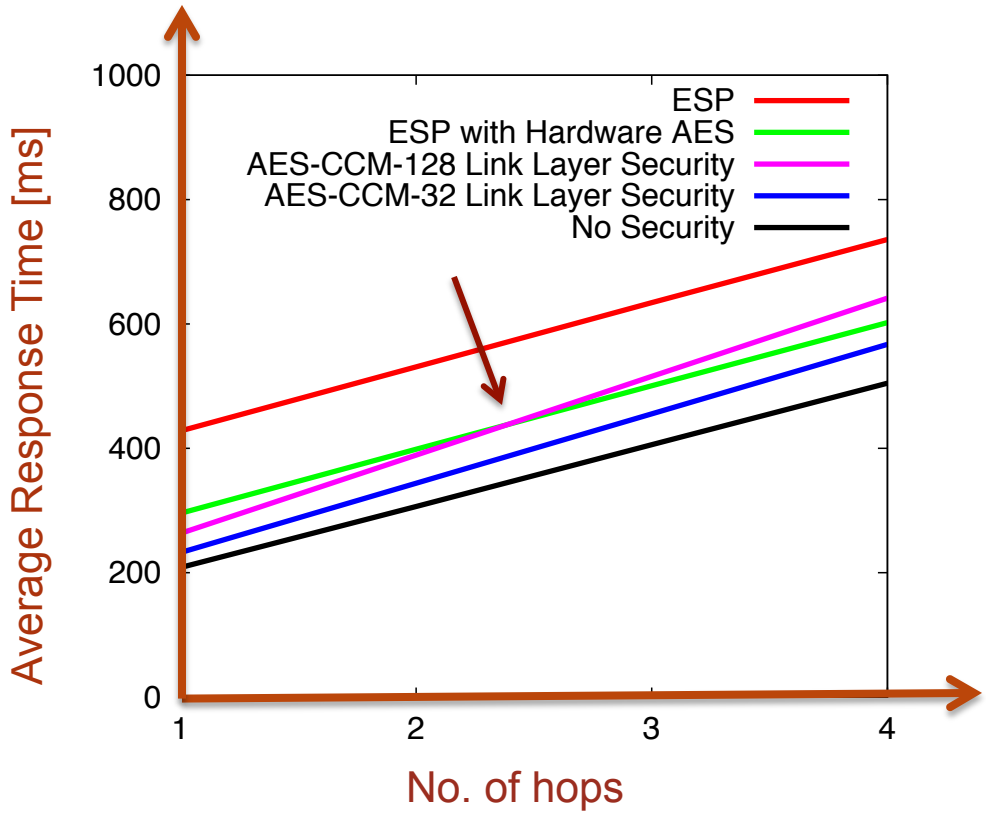
IP Datagram secured with AH



Compressed IP Datagram secured with compressed AH

IPsec vs. IEEE 802.15.4 security

- Multi hops with 512 byte data size with AES CCM



Shahid Raza, et al., *Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN.* **Journal of Security and Communication Networks, 7(12), December 2014**

Questions/Comments

shahid@sics.se

Source Code

svn co https://contikiprojects.svn.sourceforge.net/svnroot/contikiprojects/sics.se/ipsec ipsec