Cryptographically Generated Addresses (CGA) Light

draft-ev-6man-CGA-light-01

Eduard Vasilenko vasilenko.eduard@huawei.com

Problem and Solutions

[ND Trust Model] section 4.1
“Non-router related threats”:

- A malicious node could answer DAD for any request of a legitimate node
  (denial of service attack)
- A malicious node could poison the cache of another node (especially the router) to intercept traffic directed to another node
  (man in the middle attack)

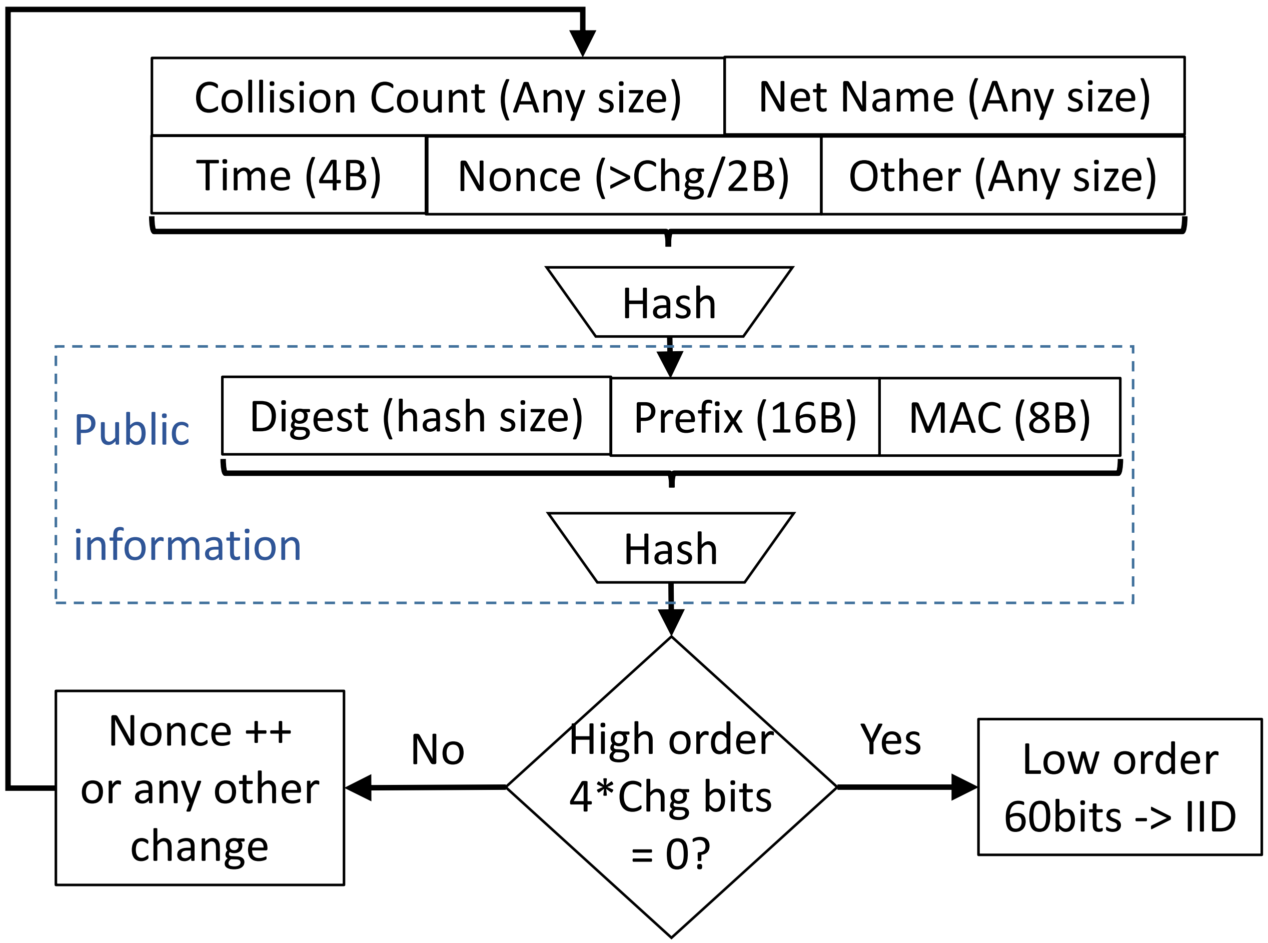
That leads to Man-in-the-middle attacks
(draft-vasilenko-6man-nd-mitm-protection):

- Rewrite cache by unsolicited NA
- Be the first and suppress DAD
- Win the race just after DAD

- IPSec was initially supposed as the solution
  Then [SEND] has been positioned for it
- [CGA] is dependent on [SEND] not a separate solution
- [SEND] has low adoption on the market for the same reason as IPSec: key management (certification authority, public key infrastructure, **trust anchor) is difficult to organize**

- Blockchain has shown value
  under the **absence of a trust anchor**
- IP to MAC mapping is the primary function of [ND]
  it could be protected with cryptography assurance
- **Security at ND may be as good**
  as security at the link layer
  (that is typically protected by encryption)

IPv6 IID generation by node (“mining IID”)



- “u” and “g” bits are deprecated (RFC 7136). Hence, all 64bits are available.
- Chg parameter occupies 4 high order bits of IID (different levels of security is possible for different nodes/interfaces on the same link).
  Hence, the IID size is 60 bits.
- Randomization is by Nonce++, Time update, fields reordering, or any other method
- IID lifetime SHOULD be limited (? years)

Mining Challenge: order of 2^(8+4*Chg+1-1) hashes

CGA Light Restrictions

Restrictions:

- Encryption could not protect against DoS or DDoS
- All nodes are equal – no possibility to restrict router functionality, RA-Guard is needed
- Intruder may claim MAC (if link-layer technology permits) then claim IP by replay attack, *but only for the disconnected node*.

Advantages/Support:

- LLA/ULA/GUA
- Different addresses per link
- Temporary MAC or IP
- Anycast for nodes on different links
- ND Proxy
- All ND extensions for far

-01 updates

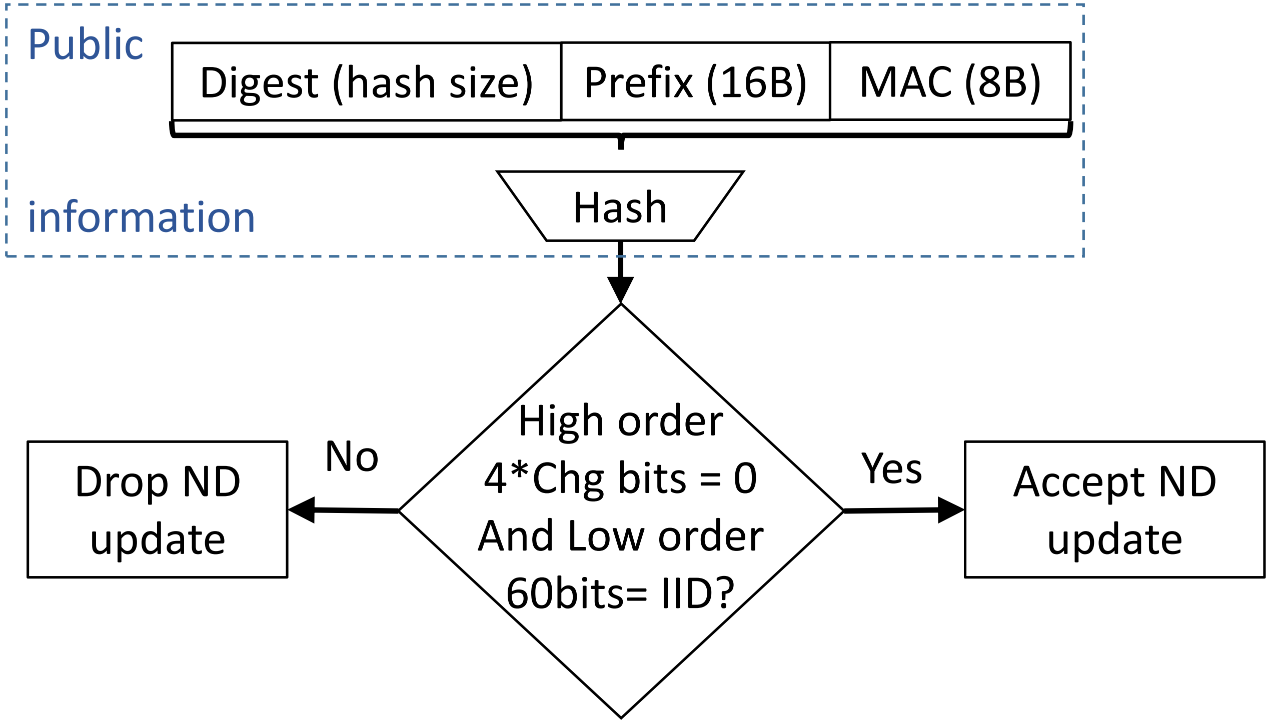
- Reference to very often cryptographic protection in L2 wireless and often cryptographic protection in L2 wireline (802.1x) in business
- Switches would block communication for duplicate addresses at L2 (flapping protection)
- Temporary MAC creates the same challenge as the temporary IP address; it would create the same load on IID generation
- Hash-Based Addresses (RFC 5535) are included in the discussion scope
- Editorial changes

- Any reviews, or criticism?
- co-authoring are welcome

Thank you

Backup Slides

IPv6 IID check by other node

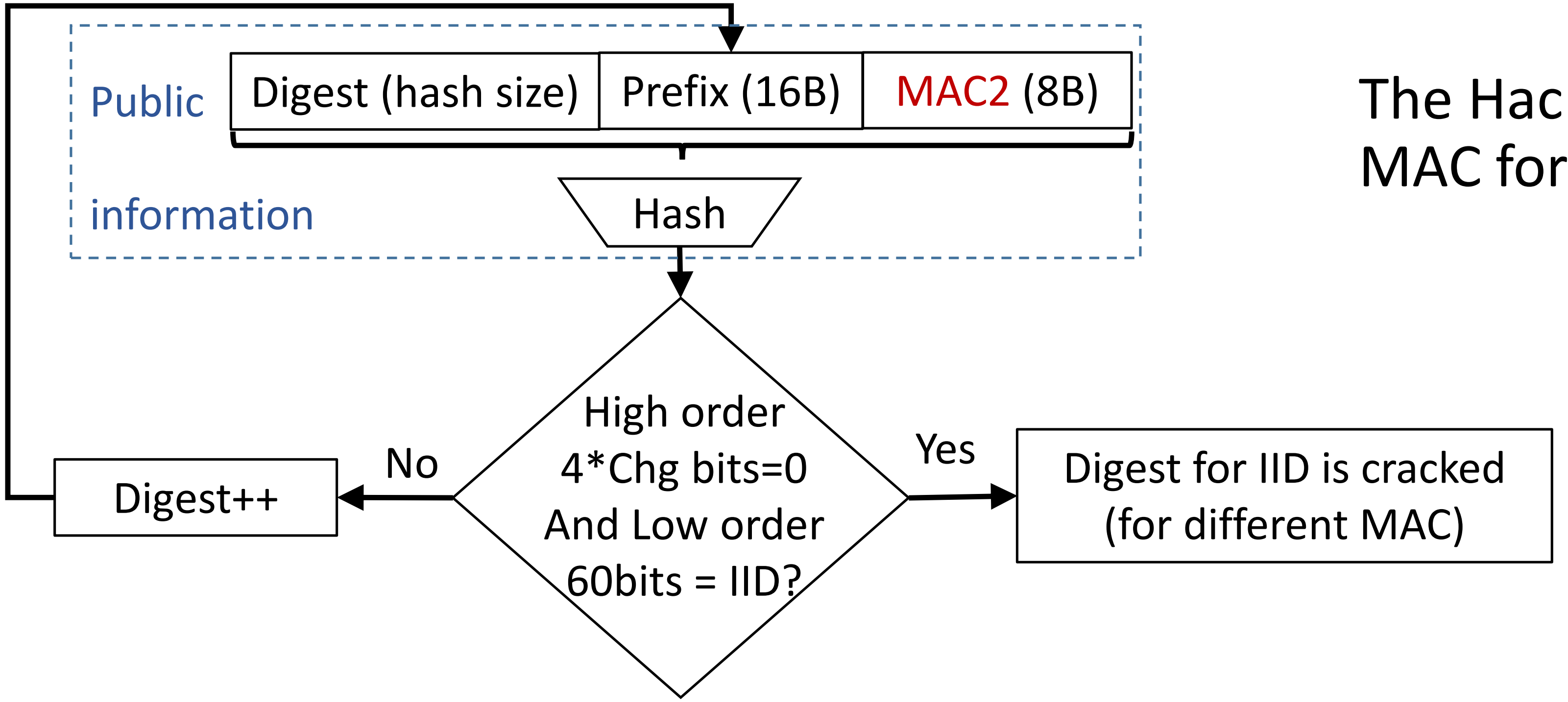


Calculated once.

Result is cached in ND.

Validation Challenge: order of 1 hash

IPv6 IID cracking by malicious node

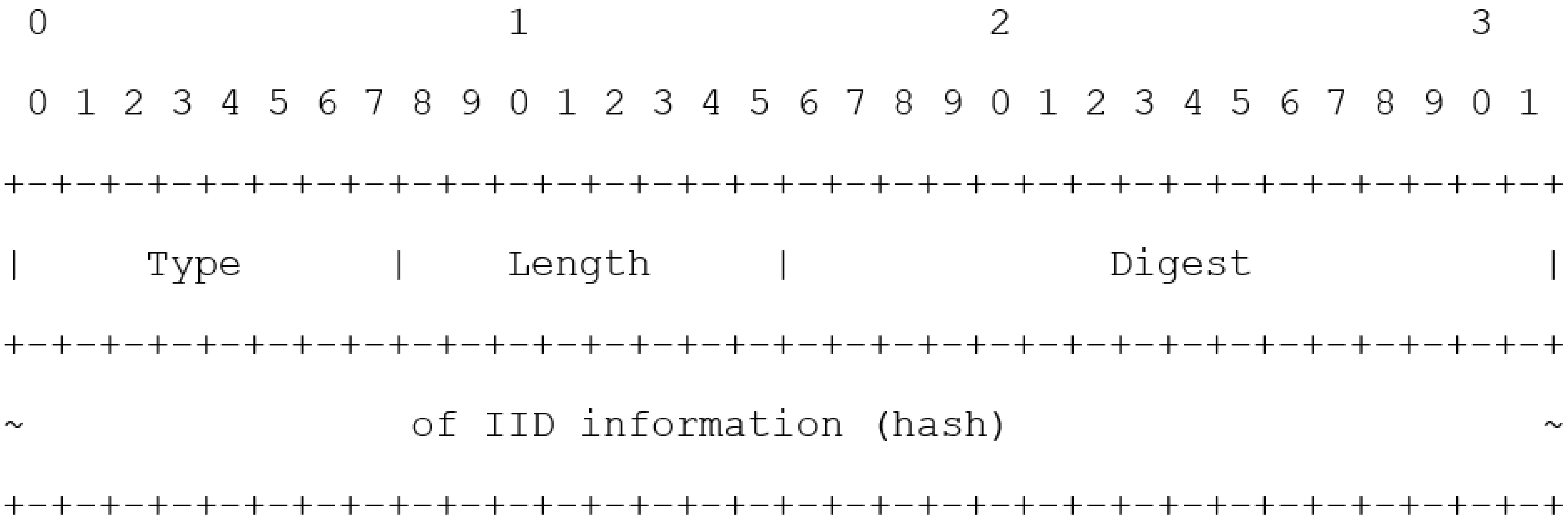

Public
information
Digest (hash size)
Prefix (16B)
MAC2 (8B)
Hash
High order 4*Chg bits=0 And Low order 60bits = IID?
No
Digest++
Yes
Digest for IID is cracked (for different MAC)

The Hacker would try to use different MAC for the legitimate host IID.

Hacking Challenge: order of 2^(8+4*Chg+60-1) hashes

ND extensions

- ND option 39 (Crypto-ID Parameters) could be reused for the hash type signaling
- Option “Digest of IID information” is needed:



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |             Digest            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                of IID information (hash)                      ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```