Cryptographically Generated Addresses (CGA) Light

draft-ev-6man-CGA-light-00

Eduard Vasilenko vasilenko.eduard@huawei.com

Problem and Solution

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

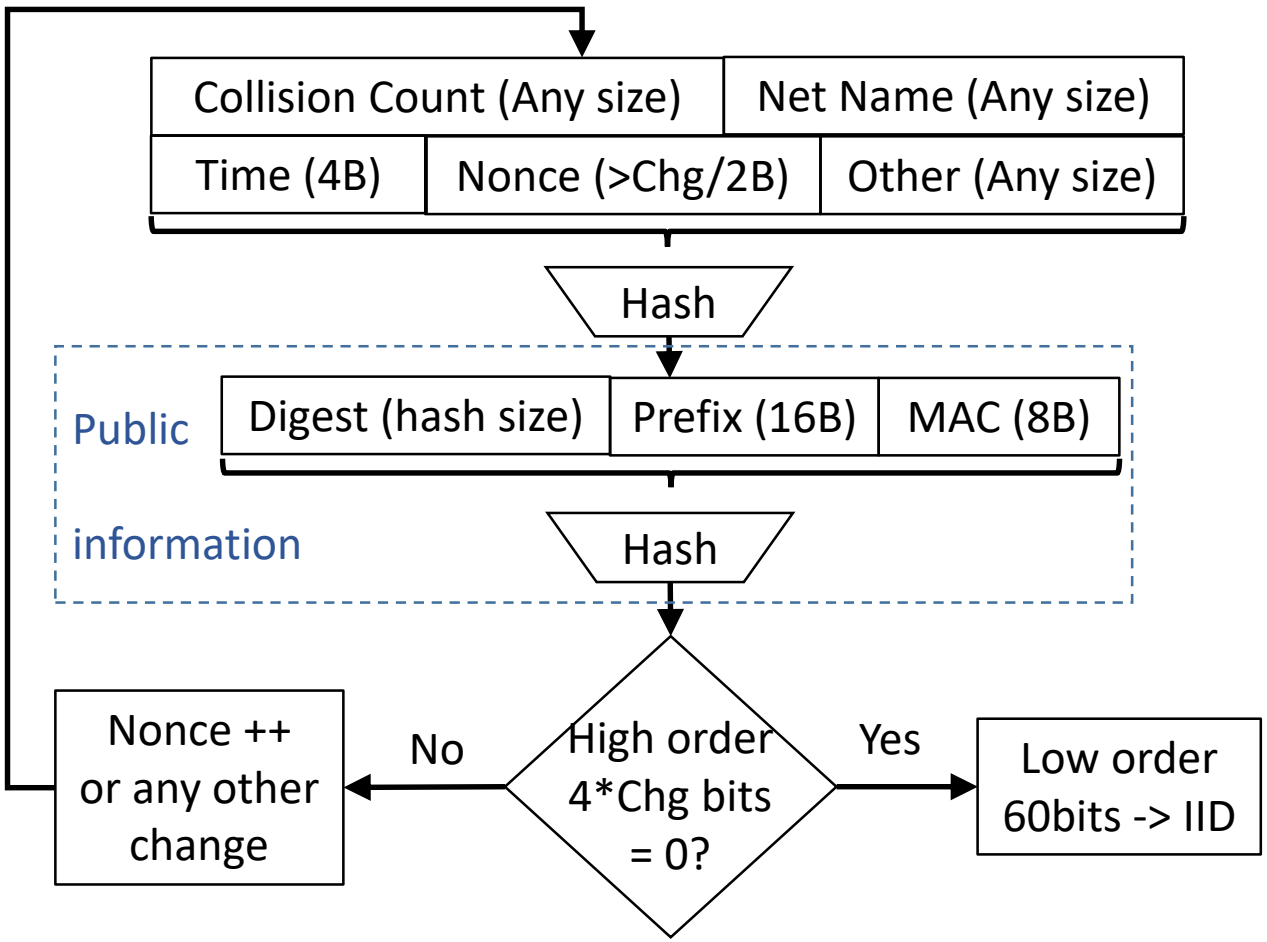
- A malicious node could answer DAD for any request of a legitimate node
  (denial of service attack)
- A malicious node could poison the cache of another node (especially the router) to intercept traffic directed to another node
  (man in the middle attack)

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 node is dependent on anyway)
- Support for Stable/Temporary/Different_per_link addresses

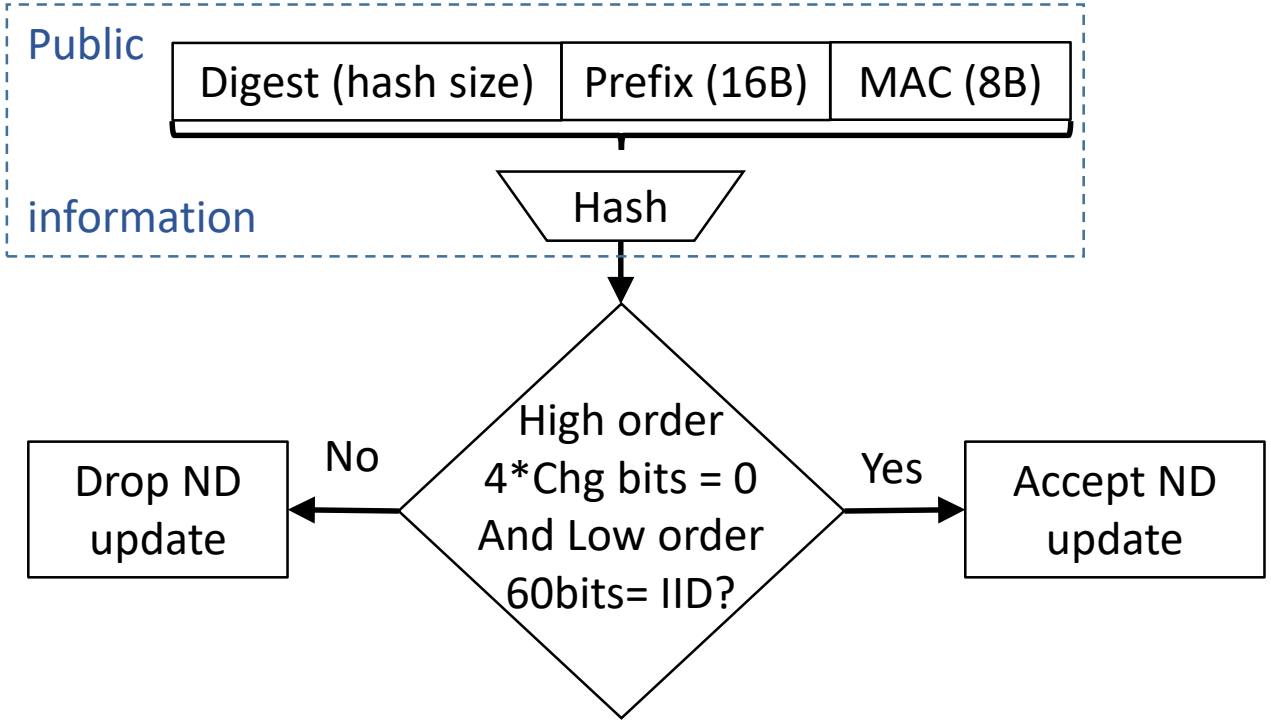
IPv6 IID generation by node (“mining IID”)



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

- IP is cryptographically tied to MAC (impersonation protection)
- Chg parameter occupies 4 high order bits of IID (different levels of security is possible for different nodes/interfaces on the same link)
- “u” and “g” bits are deprecated (RFC 7136). Chg is 4 bits. 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)

IPv6 IID check by other node

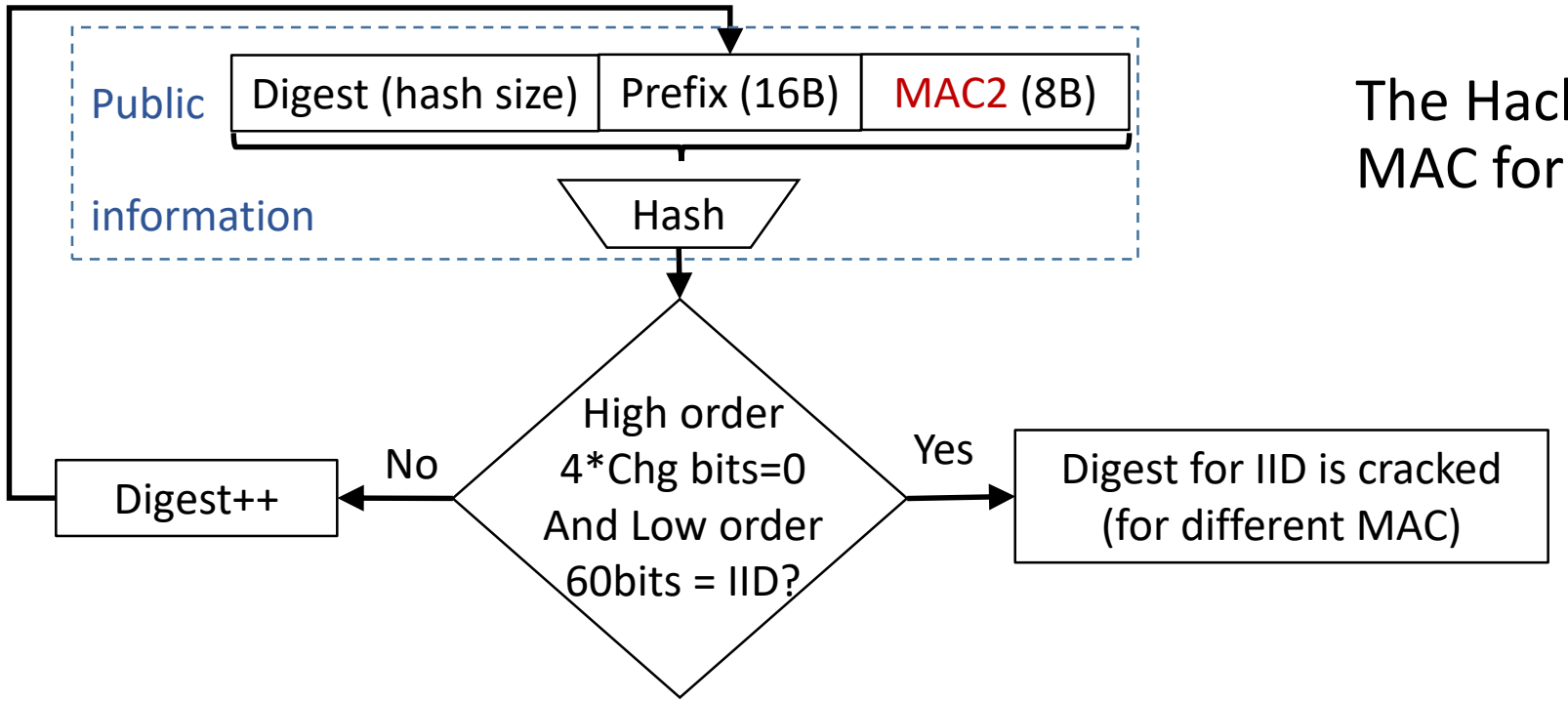


Calculated once.

Result is cached in ND.

Validation Challenge: order of 1 hash

IPv6 IID cracking by malicious node

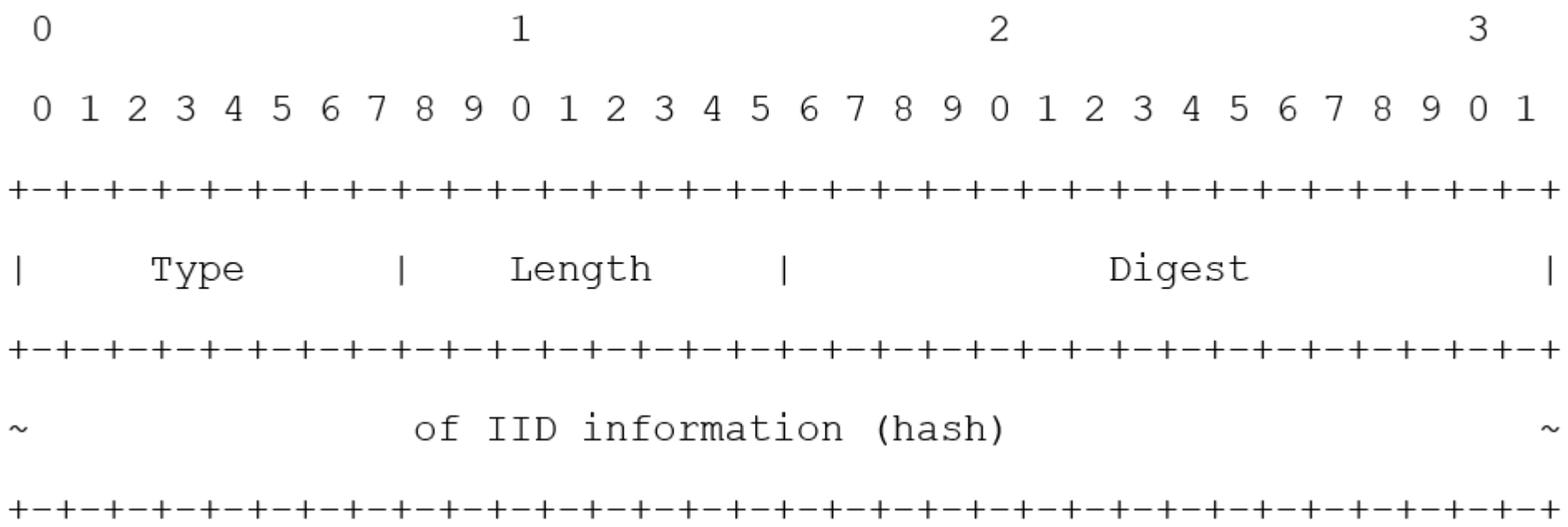


The Hacker would try to use different MAC for the legitimate host IID.

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:



CGA Light Restrictions and Next Steps

Restrictions:

- All nodes are equal – no possibility to restrict router functionality, [RA-Guard] is needed
- DoS and DDoS are still possible
- Intruder may claim MAC (if link-layer technology permits) then claim IP by replay attack
  but only for the missing/disconnected node.

Support:

- LLA/ULA/GUA
- Anycast for nodes on different links
- ND Proxy
- All ND extensions for far

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

- Thank you