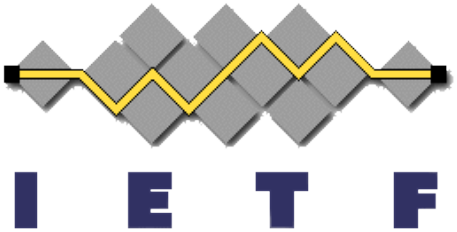


Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

A Simple Secure Addressing Scheme for IPv6 AutoConfiguration (SSAS)

draft-rafiee-6man-ssas

Authors:

Hosnieh Rafiee

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, Germany

IETF88

6man WG

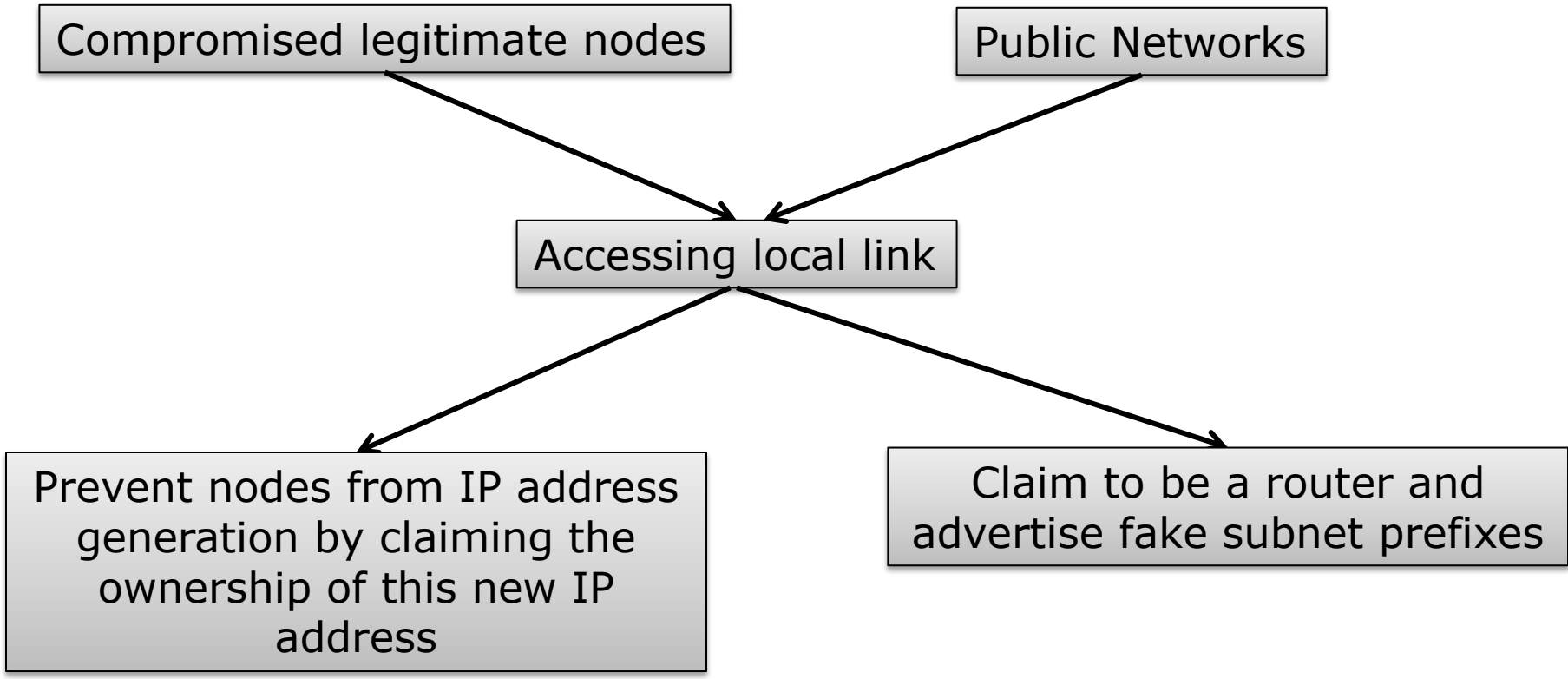
Vancouver

November 4, 2013

What is SSAS?

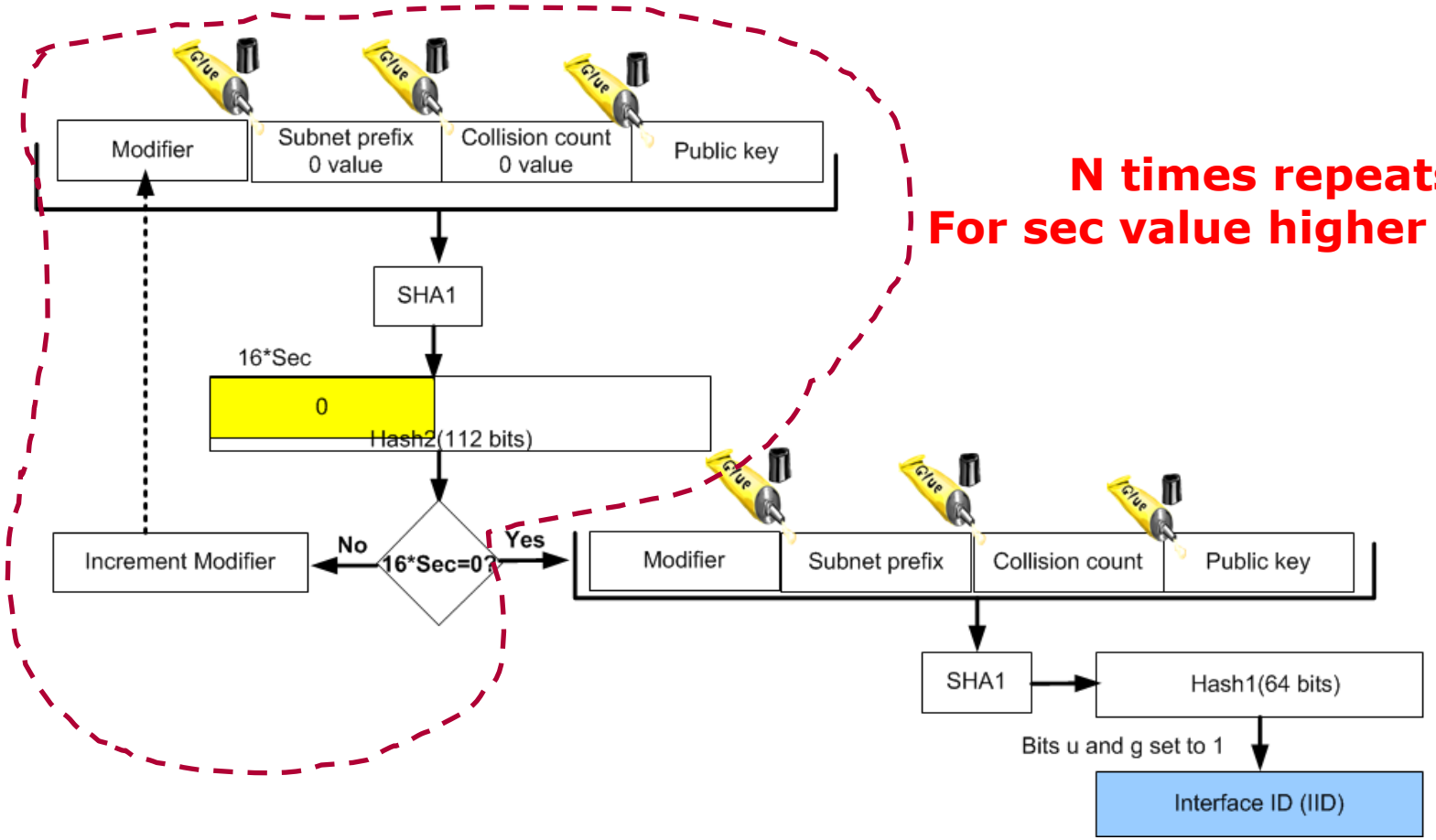
- SSAS simplify the IP address generation for the nodes
- Secure the nodes in the local link
- Provide the proof of IP Address Ownership
- How??
  - The direct use of the public key in IID generation
  - The use of ECC (RFC 6090) rather than RSA in order to decrease the packet size by a factor of 11
  - Storing the public key and MAC address in neighboring cache
  - Since it is fast, it is also ideal for nodes with limited resources

Why do we need local security



Is there any standard available?

- Prove the IP address ownership
- Use SHA-1 algorithm on public key, modifier,etc



Compare Security of SSAS and CGA

- Why SSAS can use the whole security of public key?
- For the **first time a node** joins a new network:
  - The attacker needs to do brute force attacks against **64 bits,** for CGA sec value 0 it is 59 bits. (a few seconds)
- **After the first time:**
  - The whole security of the public key

Compare Security of SSAS and CGA - II

- **Why?**
  - The node stores the public key of new node in its neighboring cache (After successful verification process)
  - Include the old public key when changes IP address and sign link layer address with old private key
  - It also used a new proposed RPKI based on the centralized RPKI in RFC 6494 and RFC 6495

- Does 6man wants to adopt this draft?