Using SEND Signature Algorithm Agility and Multiple-Key CGA to Secure Proxy Neighbor Discovery and Anycast Addressing

Tony Cheneau & Maryline Laurent
présenté par Kheira Bekara

Télécom SudParis - Département LOR - Laboratoire SAMOVAR (UMR 5157)
email: prenom.nom@it-sudparis.eu

18 mai 2011

Plan

Contexte de l'article

- pénurie d'adresse IPv4 de plus en plus concrète
  - blocs d'adresses de l'IANA épuisés (février)
  - blocs d'adresses de l'APNIC épuisés (avril)
- transition vers l'IPv6 lente mais désormais inéluctable
  - fiabilité des implémentations actuellement peu testée
  - besoin d'étudier la robustesse des nouveaux protocoles
    - DHCPv6, MIPv6, IPSEC, ...
    - protocole de découverte de voisins

Contexte de l'article

- pénurie d'adresse IPv4 de plus en plus concrète
  - blocs d'adresses de l'IANA épuisés (février)
  - blocs d'adresses de l'APNIC épuisés (avril)
- transition vers l'IPv6 lente mais désormais inéluctable
  - fiabilité des implémentations actuellement peu testée
  - besoin d'étudier la robustesse des nouveaux protocoles
    - DHCPv6, MIPv6, IPSEC, ...
    - protocole de découverte de voisins

Plan

Rôle du protocole de Découverte de Voisins (NDP) au sein de la suite de protocoles IPv6

- défini dans le document RFC 4861
- joue un rôle centrale pour la découverte du voisinage
- remplace et étend le protocole ARP utilisé en IPv4
- utilise des messages ICMPv6 (couche réseau)
- repose sur l'usage des adresses de groupe (multicast)
- portée restreinte au lien (premier saut)

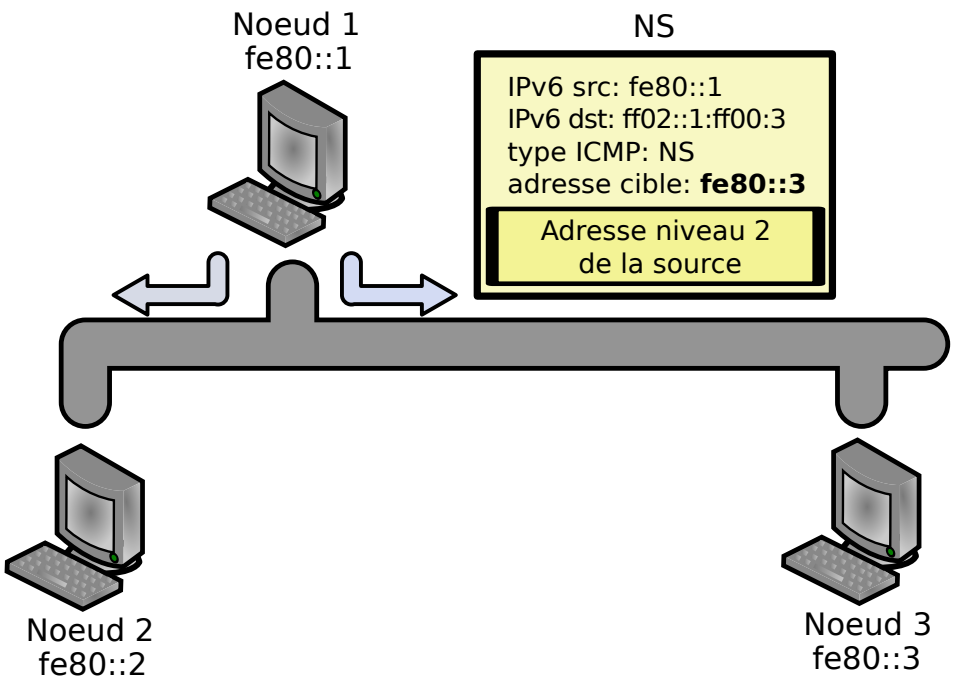
Nouveaux messages et options du protocole de Découverte de Voisins

5 messages ICMPv6 réalisent l'ensemble des fonctionnalités du NDP :

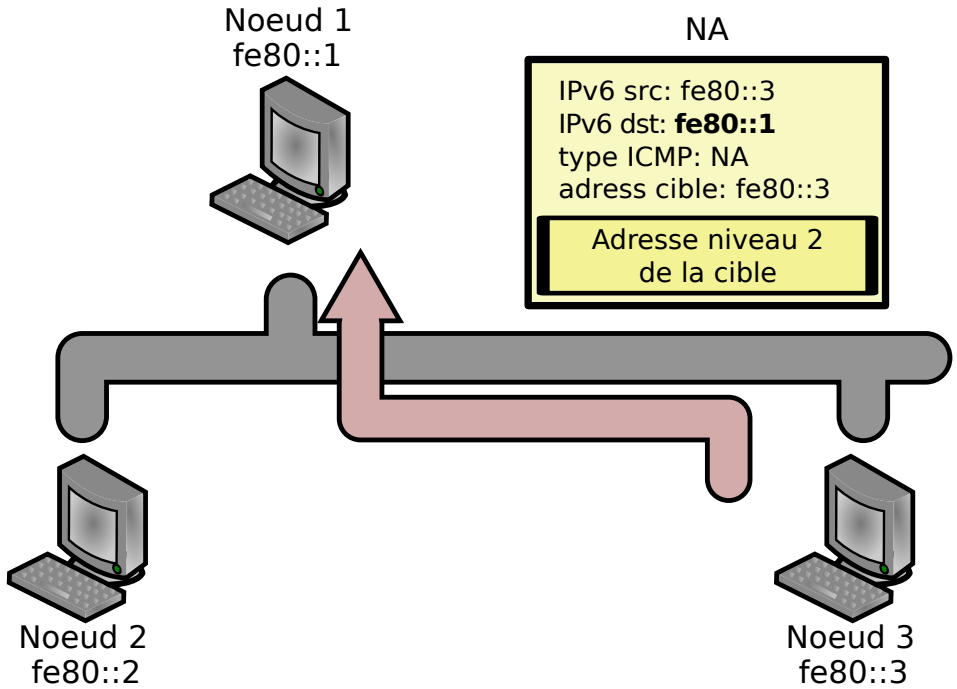
- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA), réponse à un message NS
- Router Solicitation (RS)
- Router Advertisement (RA), réponse à un message RS
- Redirect

Fonctionnalité du NDP - Résolution d'Adresse

L'initiateur de la requête envoie un message *Neighbor Solicitation* :

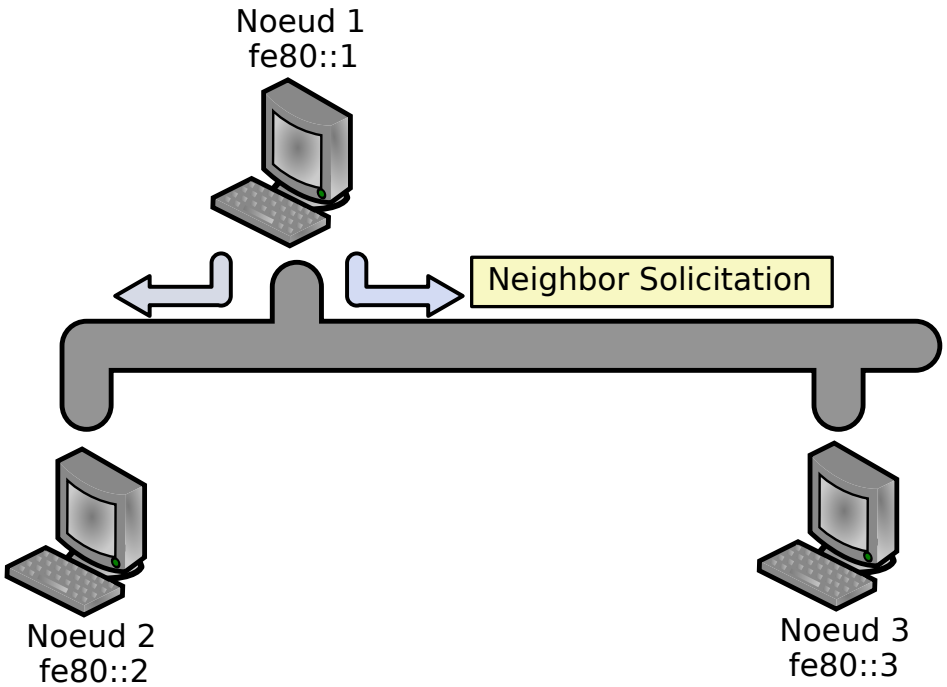


La cible répond par un message *Neighbor Advertisement* :

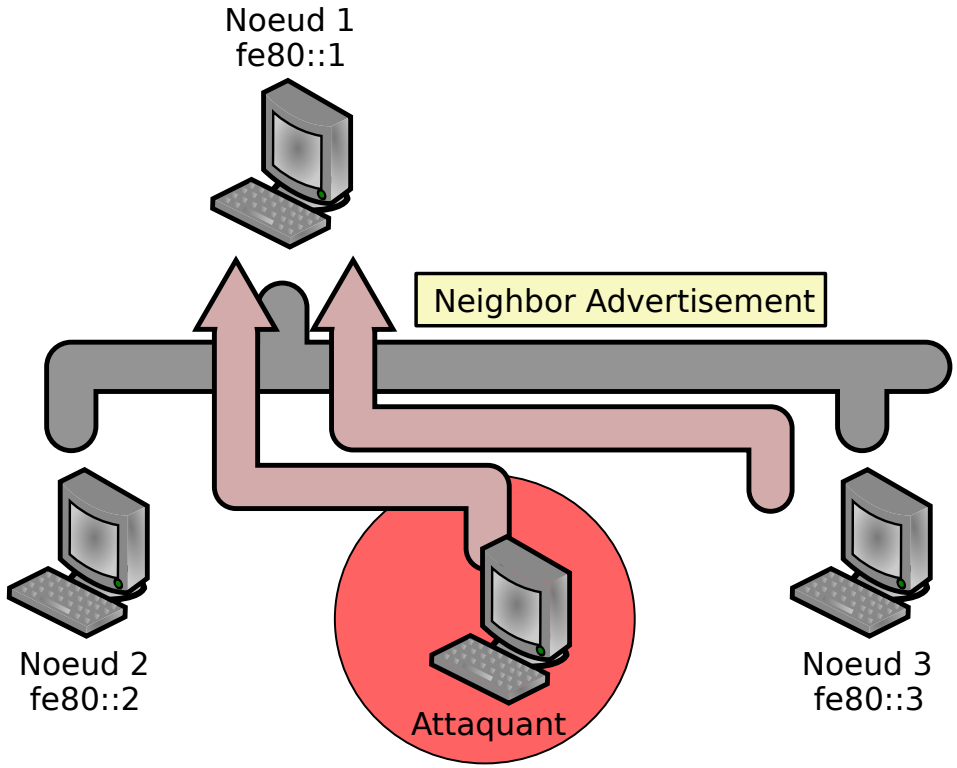


Attaque par usurpation d'adresse

La victime envoie un message *Neighbor Solicitation* :



L'attaquant répond par un faux message *Neighbor Advertisement* :



Vulnérabilité du NDP et classification des attaques

- aucune protection par défaut sur les messages NDP
- la majorité des attaques du protocole ARP s'appliquent au NDP
- attaques classifiées dans le document RFC 3756 :
  - attaques liées au routage (par ex. déni de service sur le routeur par défaut)
  - attaques non liées au routage (par ex. usurpation d'adresse)
    - attaque par usurpation d'adresse
    - attaque par déni de service sur la procédure de DAD
    - ...
  - attaques par rejeu de messages
  - attaques depuis l'extérieur

Le Secure Neighbor Discovery protocol (SEND)

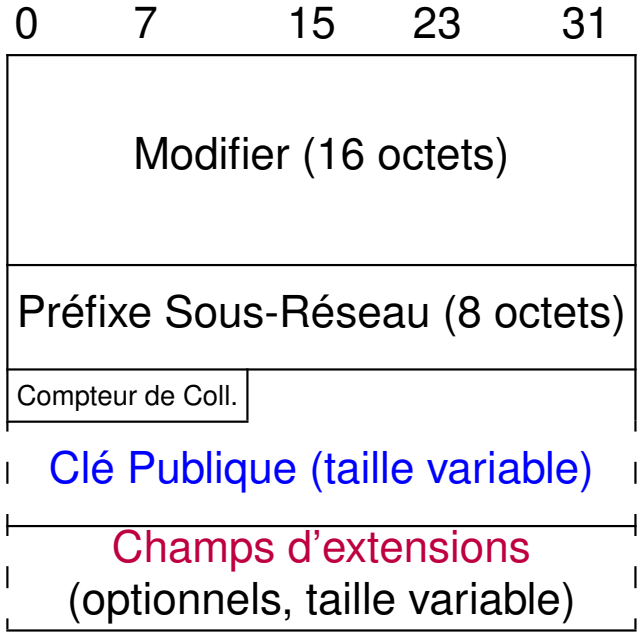
- défini dans le document RFC 3971
- couvre deux aspects :
  - protège contre l'usurpation d'adresse
  - prouve l'authenticité des routeurs d'accès
- dans la pratique, protection appliqué aux messages ICMPv6 du NDP
- fortement lié aux nouvelles adresses IPv6 CGA

Options et messages définis dans SEND

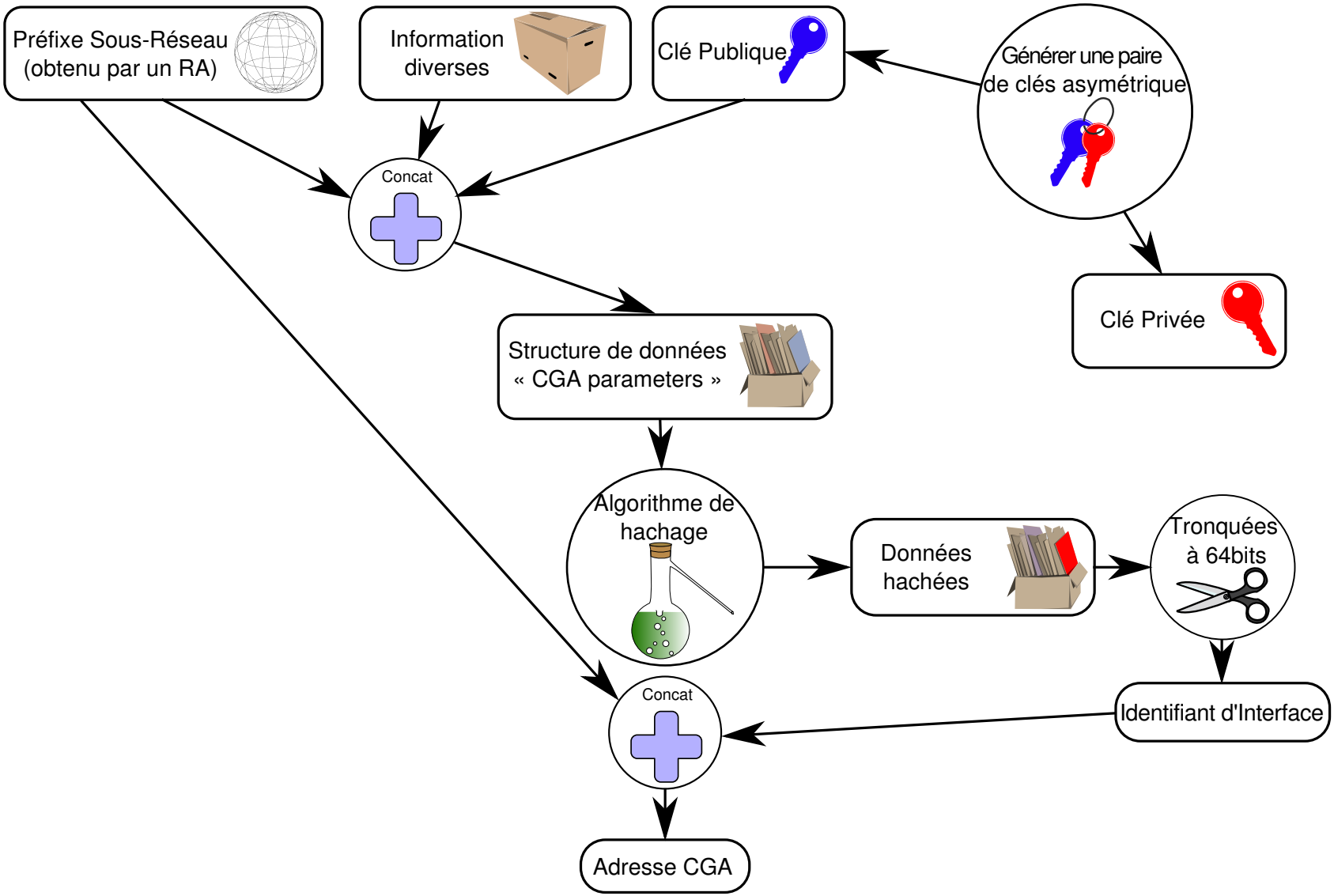
- à chaque message, SEND joint les options suivantes :
  - horodatage (anti-rejeu)
  - nonce (anti-rejeu)
  - option CGA (pour la vérification de l'adresse)
  - option de signature RSA (preuve de possession de l'adresse)
- deux nouveaux messages permettent de valider les routeurs :
  - Certificate Path Solicitation
  - Certificate Path Advertisement

Les Cryptographically Generated Addresses (CGA)

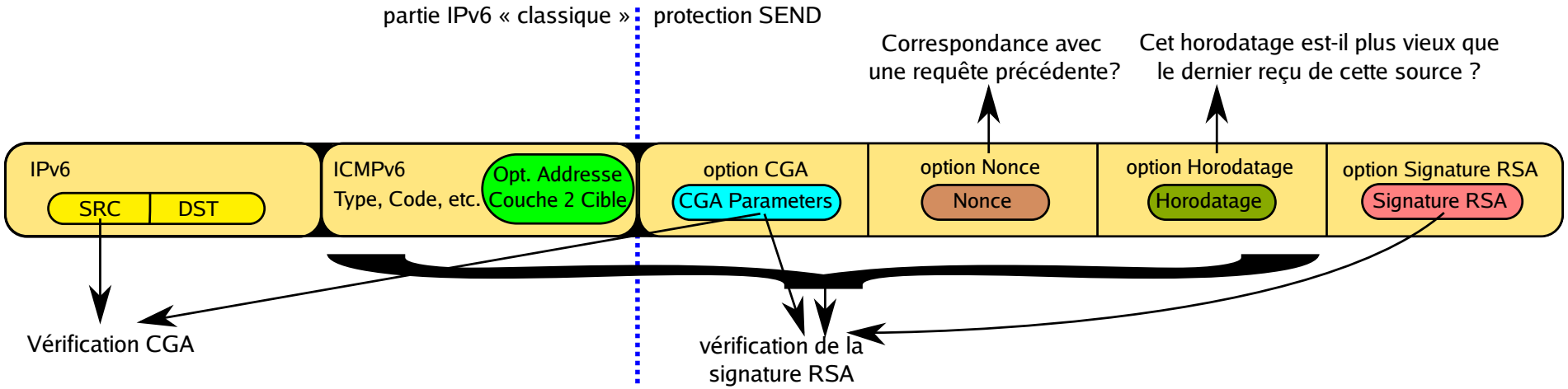
- dérivées du concept des identifiants SUCV
- lient une clé publique (ainsi qu'un ensemble de paramètres publics) à une adresse IPv6 au travers d'une fonction de hachage (SHA-1)
- reposent fortement sur la structure de données *CGA Parameters*
- format indépendant du type de clé



Mécanisme de génération d'une adresse CGA



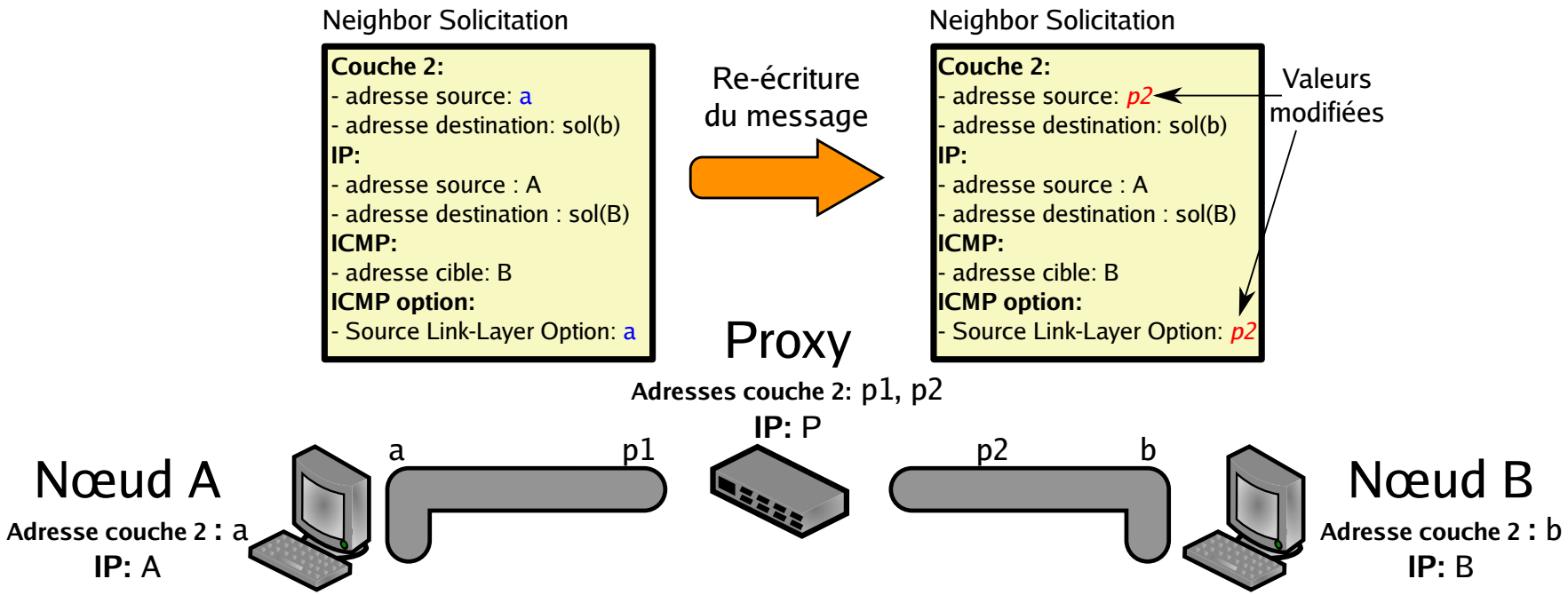
Message Neighbor Advertisement protégé par SEND



Plan

Proxy Neighbor Discovery (Proxy ND)

- trois types de Proxy Neighbor Discovery :
  - *Proxy Neighbor Advertisement* (RFC 4861)
  - *Mobile IPv6* (RFC 3775)
  - *Neighbor Discovery Proxies* (RFC 4389)
- modèle opératoire incompatible avec SEND :
  - crée de nouveaux messages à la place du nœud propriétaire de l'adresse
  - modifie les messages ICMPv6 en vol



Adressage anycast

- défini dans le document RFC 4861 :
  - plusieurs nœuds sur un même lien partagent une adresse
  - géré via l'ajout d'un délai aléatoire dans la réponse au message *Neighbor Solicitation*
- là encore, modèle opératoire incompatible avec SEND :
  - l'utilisation d'une même adresse implique le partage du matériel cryptographique (clé privée liée à l'adresse), ce qui compromet la sécurité de la solution (effet domino)

Solutions de partage d'adresse sécurisé pour SEND

- "Support du Proxy ND sécurisé pour SEND" :
  - actuellement favorisée à l'IETF
  - signature des messages par le proxy
  - basée sur les attributs EKU des certificats X.509
  - définie une nouvelle option dérivée de l'option *Signature RSA*
- "Délégation de droits pour l'annonce ND" :
  - autorisation du proxy par le nœud (création d'un certificat)
- "Solution à base de signature en anneau" :
  - basée sur l'algorithme Rivest-Shamir-Tauman
  - CGA composée des clés des différents routeurs

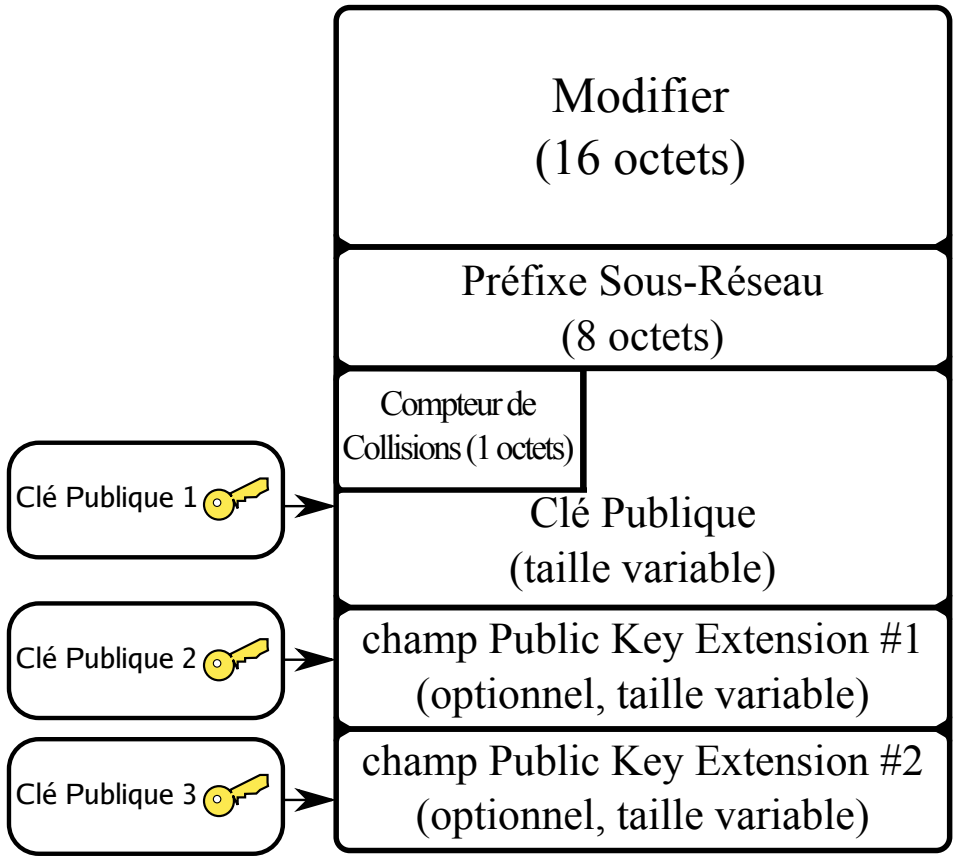
Plan

Réutilisation des travaux sur la *Signature Algorithm Agility*– rendre SEND indépendant de l'algorithme de signature

- CGA & SEND trop fortement liés à SHA-1 et RSA
- nœud à faible capacité de calcul ne supportant pas RSA
- améliorations des performances via l'utilisation de nouveaux algorithmes cryptographiques (par ex. courbes elliptiques)
- préconisation du NIST pour l'arrêt de l'utilisation de l'algorithme SHA-1

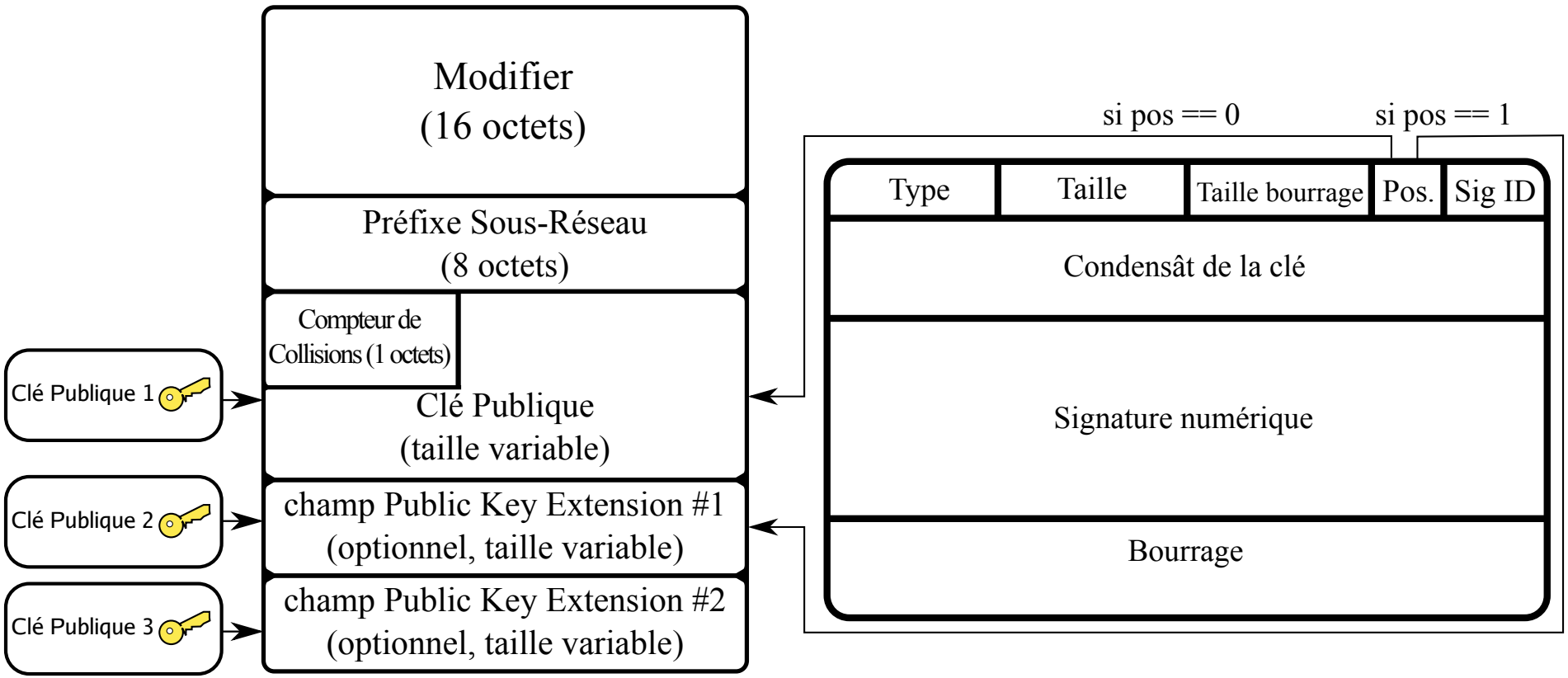
Support de plusieurs clés dans les CGA - Multiple-Key CGA (MCGA)

- définition d'une nouvelle option *Public Key Extension*
- permet le stockage de plusieurs clés publiques dans la structure de données *CGA Parameters*



Extension de l'option de signature RSA - option *Universal Signature* (US)

- clé publique liée à la signature pointée par le champ *position*



Construction d'une Multiple-Key CGA pour plusieurs nœuds

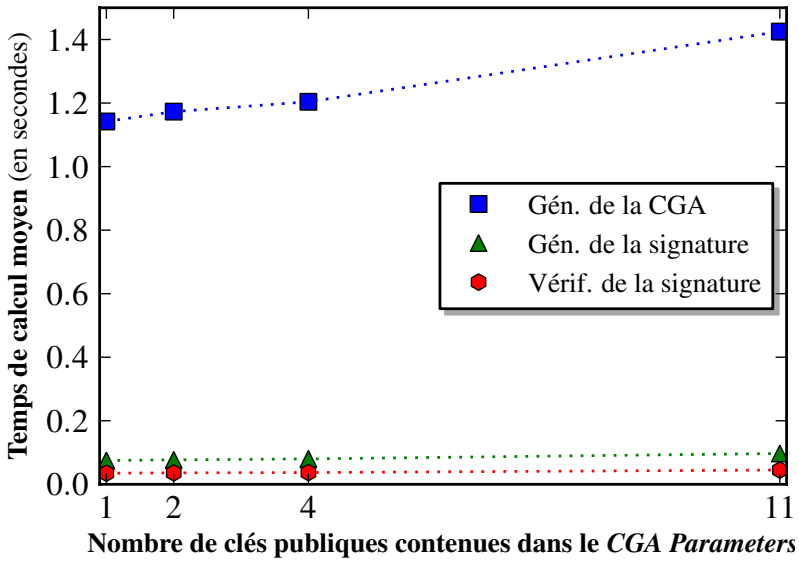
- utilisation directe des extensions de *Signature Algorithm Agility*
- apprentissage des proxy par l'intermédiaire des messages *Router Advertisement* (dans la procédure d'*Autoconfiguration d'Adresse Sans État*)
- clé publique de chaque proxy stockée dans une extension *Public Key* (*CGA Parameters*)
- avantages
  - faible modification du nœud si celui-ci supporte la *Signature Algorithm Agility*
  - autorisation du proxy par les nœuds protégés
- inconvénients
  - taille des messages du NDP croissant avec le nombre de clés
  - difficulté de l'ajout de nouveau proxy après la construction de l'adresse

NDprotector : une implémentation espace utilisateur des CGA et du protocole SEND

- née du manque d'implémentation facilement extensible
- écrie en Python (pour plus d'extensibilité)
- interopérable avec l'implémentation de référence (NTT DoCoMo)
- par la suite modifiée pour gérer les M-CGA et le partagé d'adresse anycast validé (via configuration manuelle)
- librement téléchargeable sur le site : http://amnesiak.org/NDprotector/

Performances de la solution

- (léger) impact sur la vitesse de génération d'une adresse CGA
- faible influence sur la vitesse de génération et vérification d'une signature



- croissance linéaire de la taille de la structure de données *CGA Parameters* en fonction du nombre de clés (11 clés au maximum)
- taille de la signature fixe
- pour le moment, impossible de comparer nos résultats avec les autres solutions (manque d'implémentation publique)

Limitations de la solution

- le nombre de clé maximum transporté dans la structure *CGA Parameters* limité
- niveau de sécurité de la MCGA dépendant du niveau de sécurité de la plus faible des clés
- vulnérable aux attaques de types *bidding-down* (c.-à-d. si un algorithme de signature est cassé, un attaquant peut l'exploiter pour utiliser la MCGA)
- comportement par défaut proposé : définition d'une politique locale pour interdire certains algorithmes de signature

Plan

Conclusion et travaux futurs

- solution réaliste basées sur nos travaux de *Signature Algorithm Agility* permettant un partage d'adresse sécurisé dans le protocole SEND
  - implémentation dans NDprotector
  - faible impact de la solution démontré par une étude de performances
- travaux futurs :
  - amélioration de l'apprentissage des adresses partagées dans le cas de l'anycast
  - confirmation des performances via des tests plus poussés