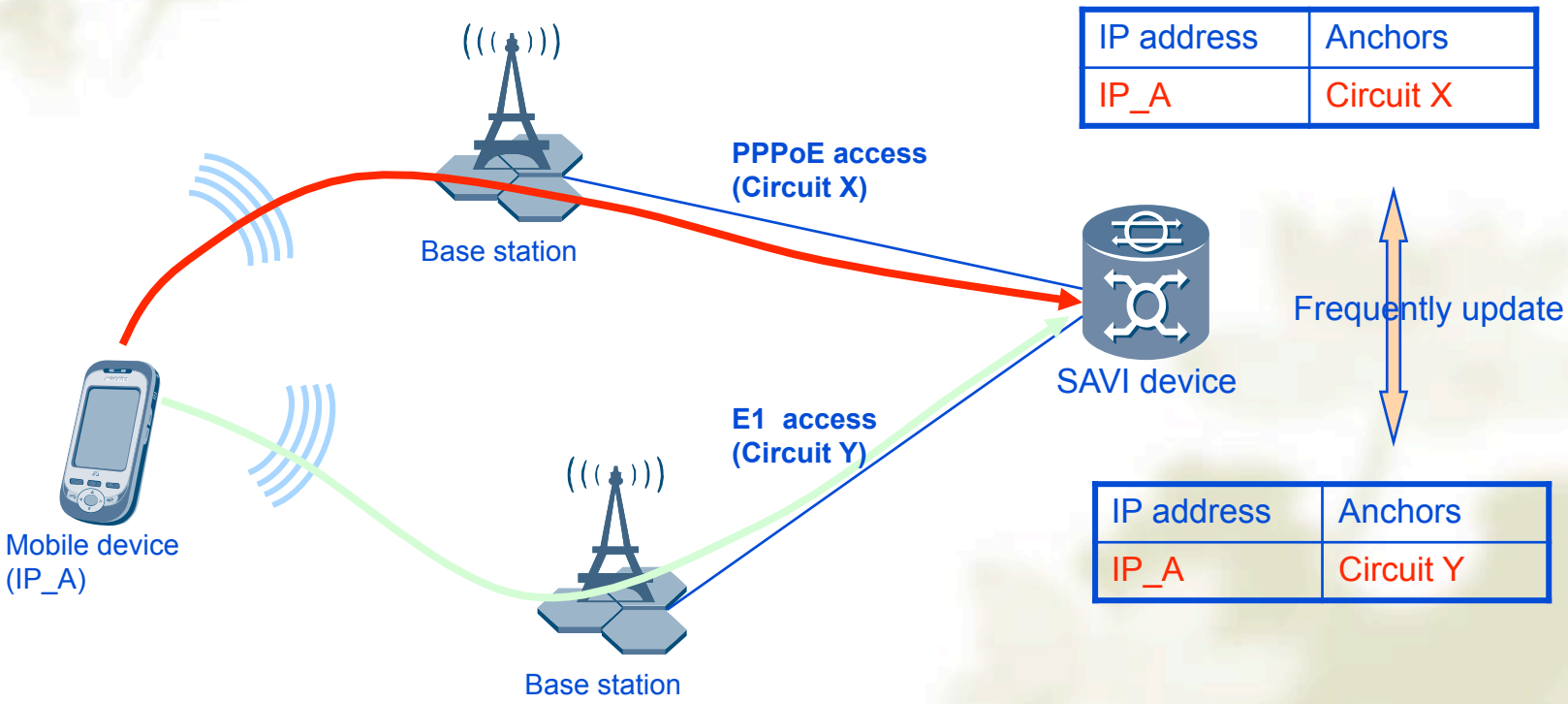
Shared Key SAVI

draft-li-savi-skey

Hongyu Li
Yizhou Li

July 2009

An example of mobile user



Problems with L2 Anchors

- Mobile user may access to the network from different L2 anchors, e.g. circuit ID, which may change frequently
- Circuit ID may vary greatly in different access networks
  - MAC
  - Ethernet Port
  - VLAN
  - E1 Time slot
  - …
- User with dual uplinks to a SAVI device
  - What anchor will be bound when the two uplinks has different circuit ID?

- **Shared key can be used as a common anchor**

Shared Key SAVI Highlight

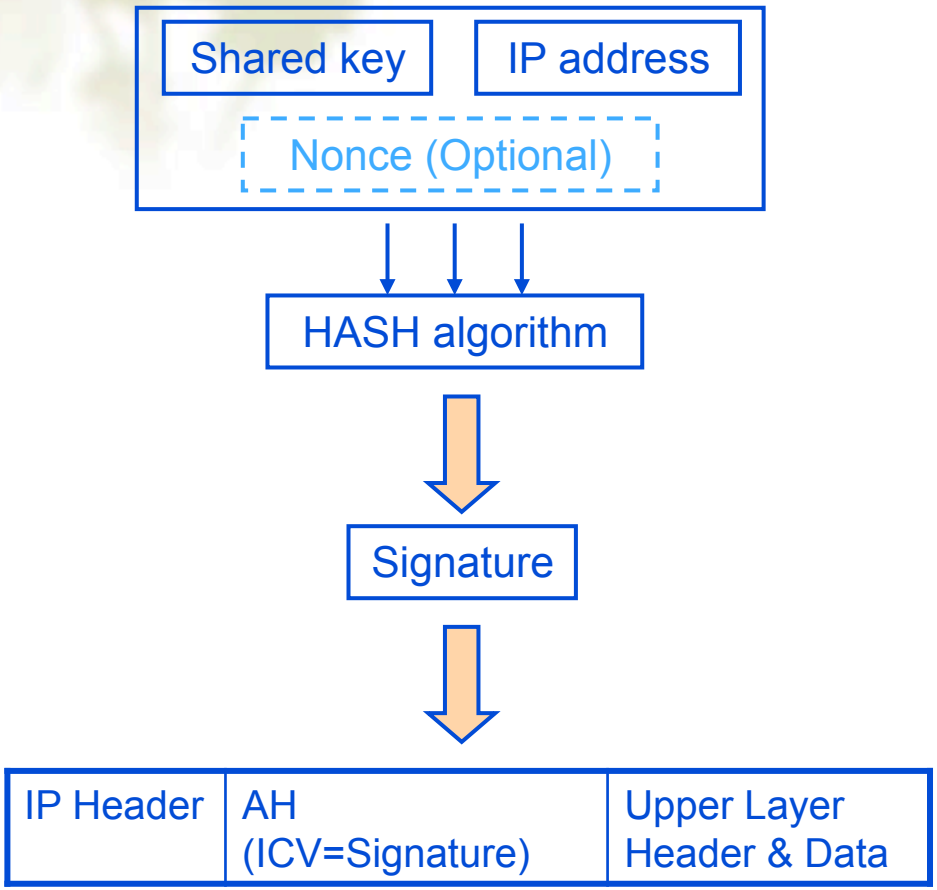
- Each host shares a key with SAVI device
- Dynamic negotiation mechanism may be used for a host to acquire a shared key
- A user is identified by its IP address
- What is used for calculating signature is only IP address but not the whole IP packet
- Signature is carried by ICV (Integrity Check Value) field in IP Authentication Header

- Validate source addresses by shared keys

SKey SAVI Data structures

- IP address entry
  - IP source address
  - shared key
  - shared key lifetime
  - hash algorithm

Processing on Host



- Host Calculate its signature from its shared key and IP address with selected HASH algorithm
- The signature is inserted in to AH's ICV field
- Sequence Number Field may be used as nonce to prevent replay attack

AH with Signature in IPv4/v6

IP Header	AH (ICV=Signature)	Upper Layer Header & Data

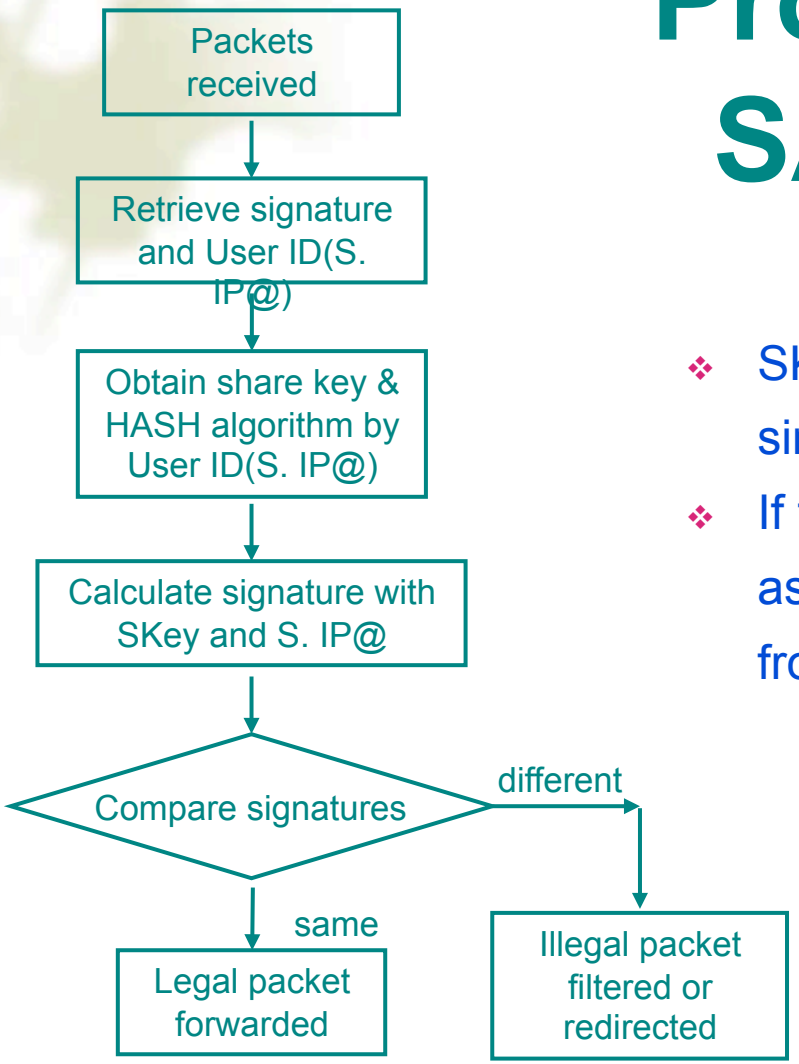
SKey signature in IPv4 packet

IP Header	hop-by-hop, routing, fragment.	AH (ICV=Signature)	Dest. option	Upper Layer Header & Data

SKey signature in IPv6 packet

- SKey SAVI is applicable to both IPv4 and IPv6
- In IPv6 context, AH is viewed as an end-to-end payload, and thus should appear after hop-by-hop, routing, and fragmentation extension headers.

Processing on SAVI Device



- SKey SAVI computes a signature in a similar way as host
- If the two signatures matches, we can assert that the IP packet was sent from the legal owner of the IP address

Advantages of SKey SAVI

- Link layer and physical layer info independent
- Applicable to both IPv4 and IPv6
- More efficient than IPsec
- SKey is more secure than L2 anchors

Next Steps?