SAVAH: Source address validation with Host Identity Protocol

Dmitriy Kuptsov, Andrei Gurtov

firstname.lastname@hiit.fi

Outline

- Address spoofing problem
- Related work
- SAVAH approach
- Implementation
- Deployment and performance evaluation
- Future work

Source address spoofing

- Routing is done using only destination IP address
  - Source IP address is not validated nor authenticated
  - Malicious users can forge nodes in the Internet
  - Gives “green” light for various attacks, such as DoS attacks
- Accounting in the Internet is not an easy thing
  - If the address was not authenticated it is hard to trace back the originator of the network communication
  - Using cryptography based authentication can solve the problem

Related work

- Currently, there are three main approaches for validating source IP address in the Internet:
  - Cryptography based validation
  - Filtering (egress/ingress)
  - “Trace back” methods
- Cryptography based solutions provide good security but require large scale deployment
- Filtering based solutions, such as ingress filtering, are easy to deploy but lack security and accountability properties
- “Trace back” approaches looks promising but still require large deployment and are less secure than the cryptography based solutions

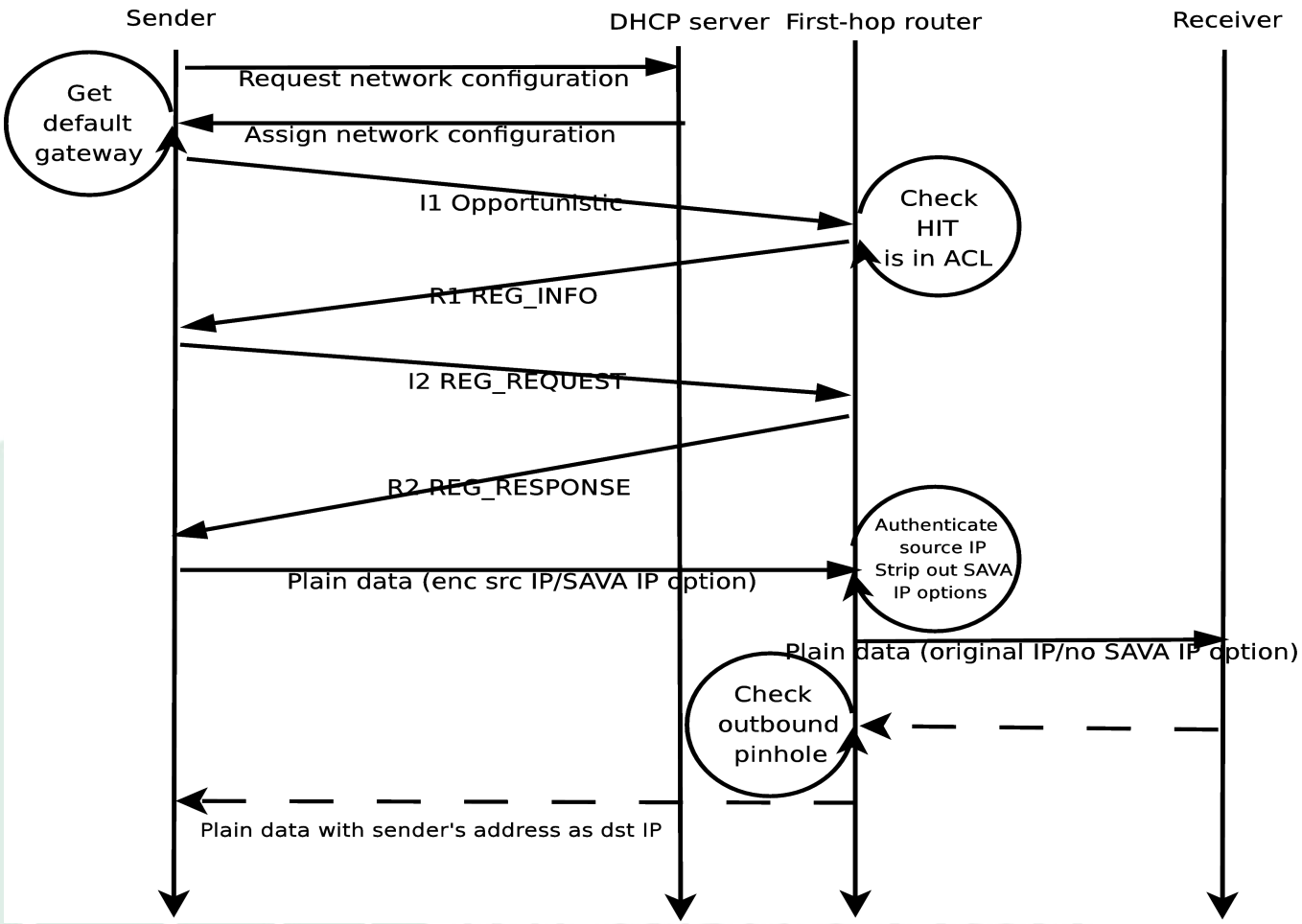
SAVAH Extension

- SAVAH: Source address validation architecture with Host Identity Protocol (HIP)
- There are two main ways to authenticate the originator of the network communication using HIP:
  - plain HIP/IPSec communication with filtering based on the list of allowed Host Identity Tags (HITs)
  - Source address authentication with HIP and SAVAH extension
- Replacement of CGA based authentication in a local area network
- The solution is suitable both for IPv6 and IPv4 networks

Pros and Cons

- Advantages:
  - Strong authentication based on cryptographic properties, can also serve to control a network access
  - Traffic accounting and malicious activity logging
  - DoS attack prevention mechanism
  - Incremental deployment, no need to modify all hosts in the Internet at once
  - In addition the user gains mobility and multihoming support
- Drawbacks:
  - Modifications of the hosts in the local network are required
  - A bit slower than regular ingress filtering, because of signature checks

SAVAH implementation



Registration with router

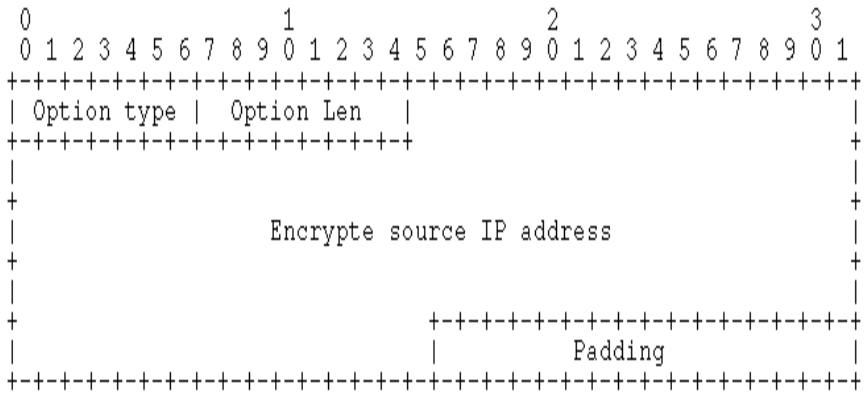
- Step 1: Locator assignment and host identifier registration
  - The host gets the locator (IP address) through one of the available mechanisms:
    - DHCP
    - Manual configuration
  - The HIT is registered (added to a list of allowed identifiers) on the first-hop router
- Step 2: The host discovers the SAVAH router
  - The identifier of router can be obtained through:
    - DHCP offer
    - Manual configuration
    - Opportunistic service discover procedure

Registration with router (continue)

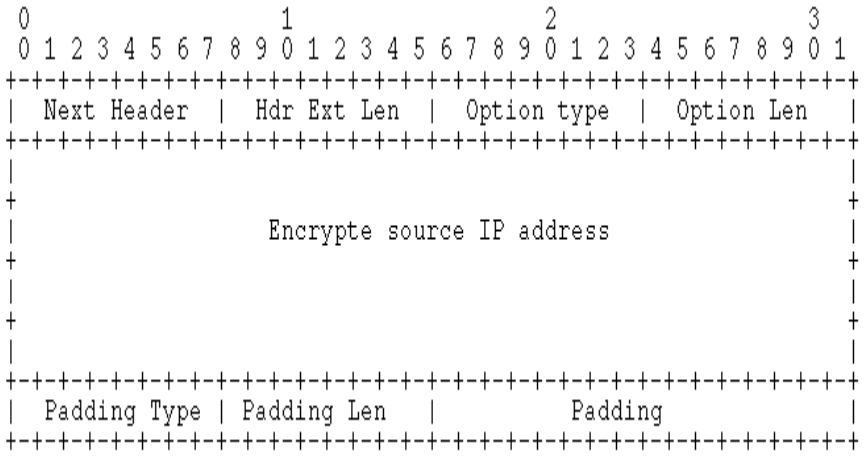
- Step 4: Registration with SAVAH service
  - Accomplished with HIP service registration procedure described in RFC 5203 “Host Identity Protocol (HIP) Registration Extension”
  - Registration succeeds if:
    - During HIP base exchange a source HIT found in signaling packets (I1 and I2) is present in the list of allowed HITs
    - After base exchange completes a database of previously seen locators (IP addresses) does not contain a record with a source IP address of a registrar

Authentication

- After SAVAH registration is completed both parties (the host and the router) posses a shared secrete key
- Host appends special IP option to each outgoing packet containing value from
  HMAC (key | source IP) operation
- Router compares the values from packet and locally calculated secure hash using shared secret key

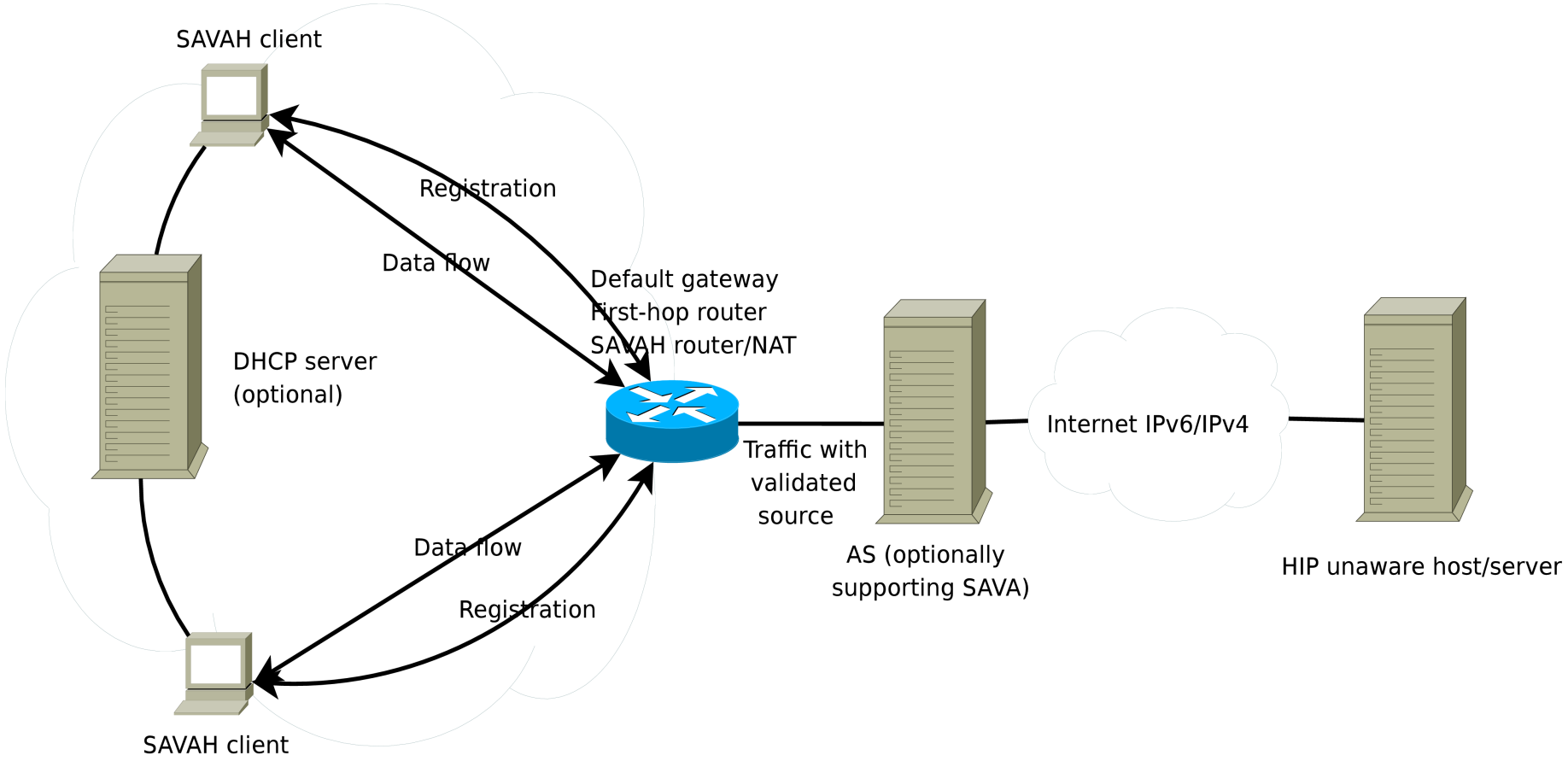


IPv4 option format

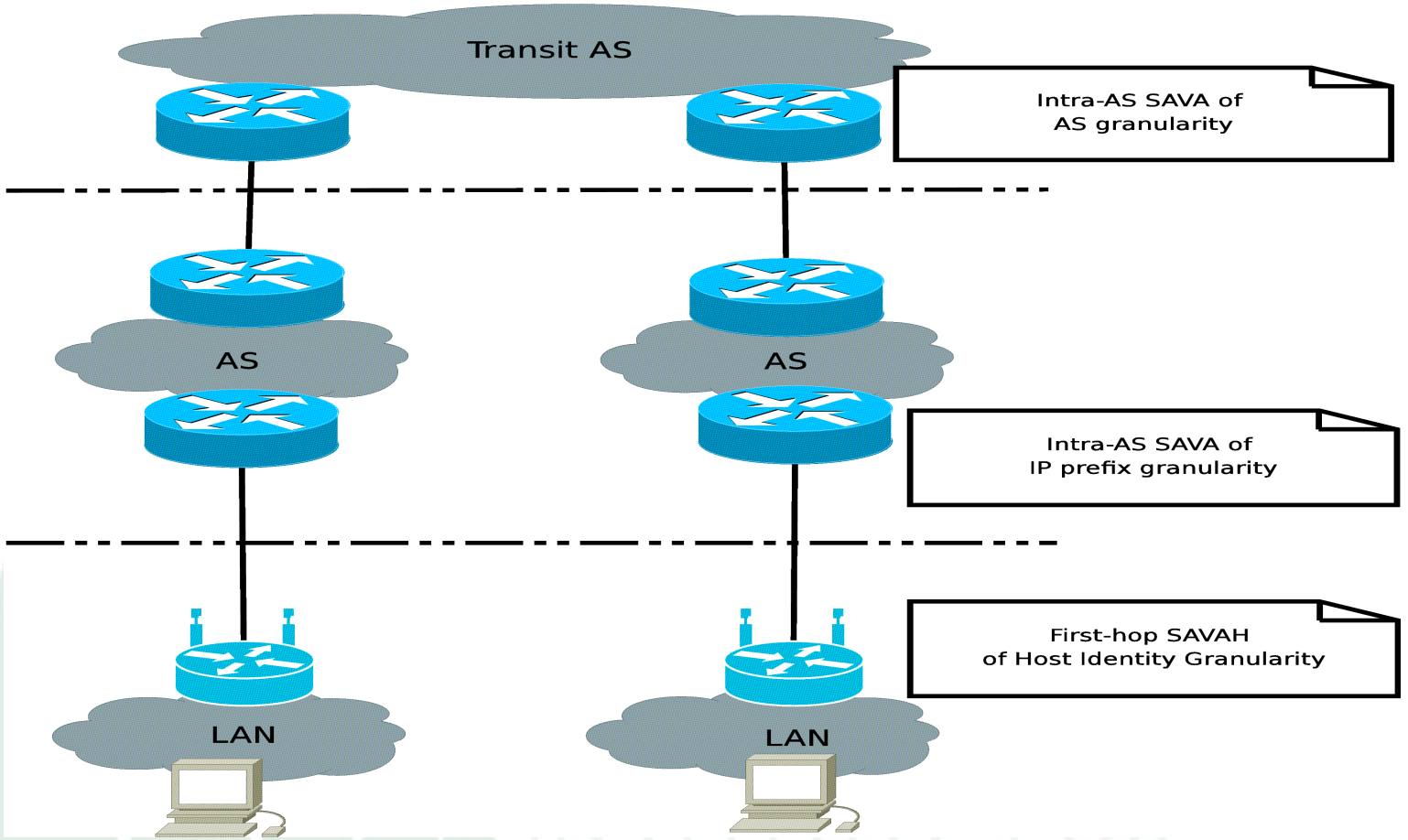


IPv6 option format

SAVAH deployment (local network topology)



SAVAH deployment (placement in the Internet)



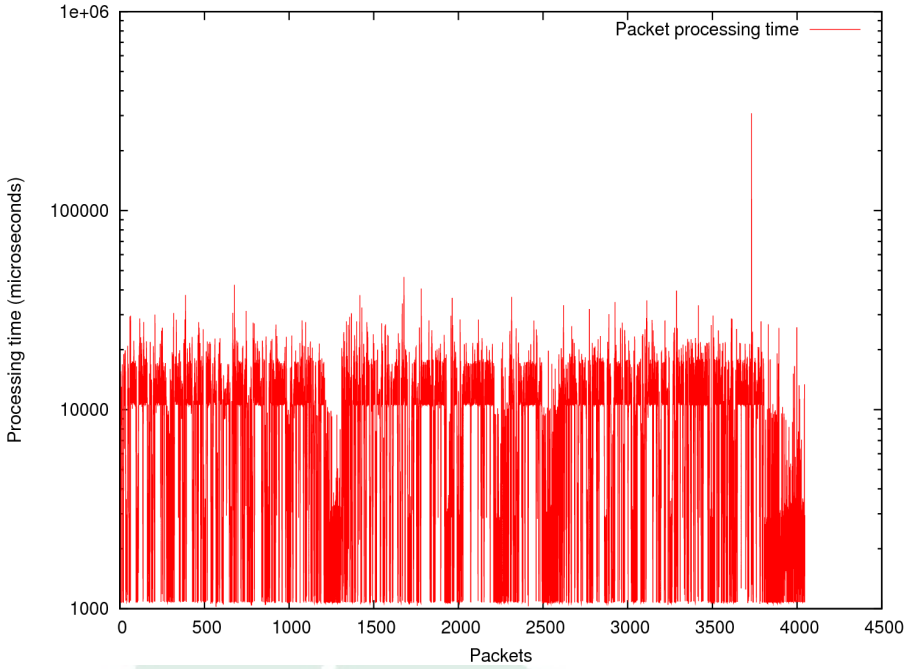
Original source “Source Address Validation: Architecture and Protocol Design”

Performance evaluation (configuration)

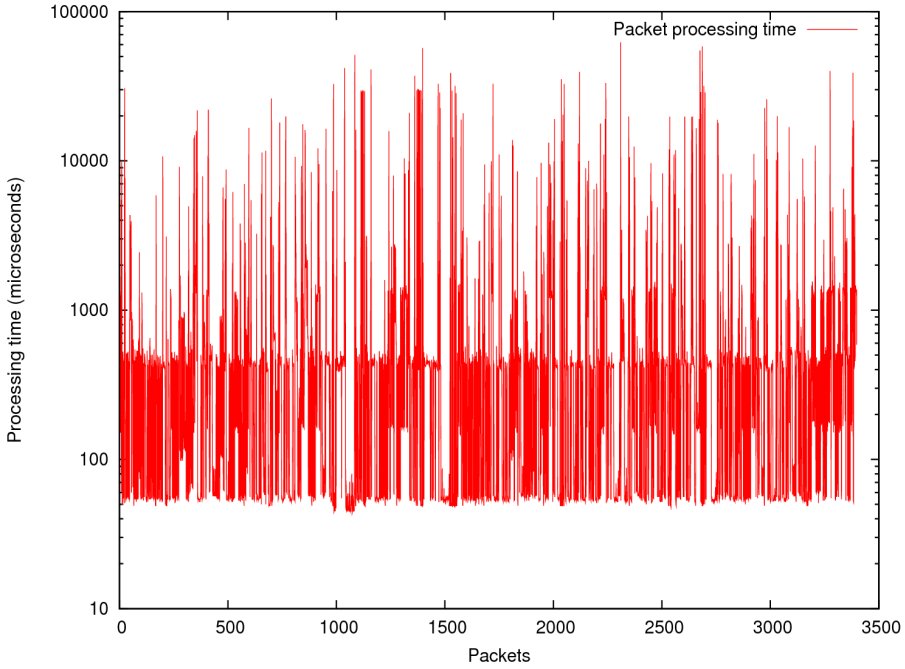
- Hardware used in the experimental setup:
  - Wireless access point (Avila board and Fonera FON2100 router) used as first-hop router and a DHCP server in our network:
    - Customized OpenWRT Linux distribution
    - CPU: 533 MHz (Avila board)
    - RAM: 128 Mb (Avila board)
  - Laptop used as SAVAH client:
    - Ubuntu Linux distribution
    - CPU: 2.4 GHz Dual Core
    - RAM: 3 Gb
- Network was configured to support both IPv4 and IPv6 stacks

OpenWrt
Wireless Freedom

Performance evaluation (results)



SAVAH packet processing time on router (Avila board)



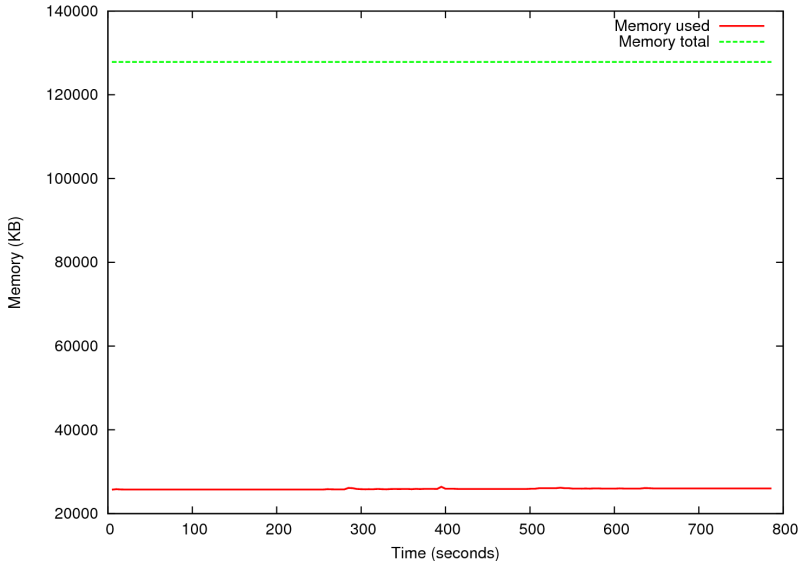
SAVAH packet processing time on client (laptop)

SAVAH router (Avila board)	9351
SAVAH client (laptop)	1324

Average processing time (microseconds)

Performance evaluation (results)

- SAVAH does not stress the device in terms of memory usage
- Around 2 MB of additional memory is occupied when running HIP in SAVAH mode



Memory usage on the SAVAH router

Future work

- Pilot the deployment of SAVAH in a large scale network
- Further research on source address validation
- Work on Internet draft related to SAVAH
- Research on the alternative solutions

Questions?

Thank you!