HIP-based P2PSIP proxy

HIP RG Meeting
70th IETF – Vancouver
Joakim Koskela

HIP-based P2PSIP

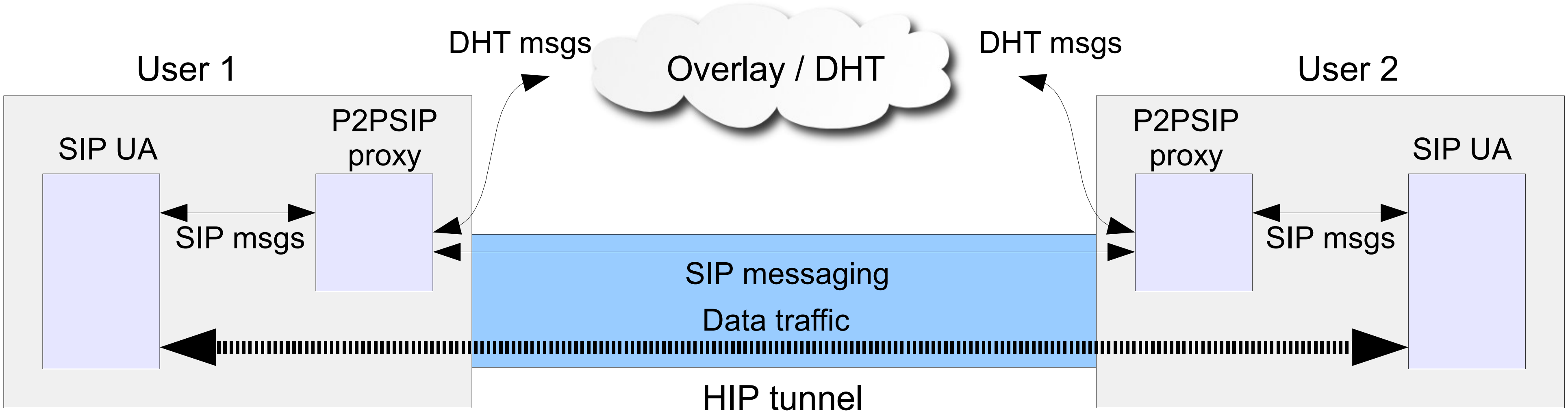
- P2PSIP in general: replace SIP server architecture with a DHT
  - Used for routing messages and locating peers & services
  - New challenges for security (confidentiality, identity theft, privacy..), connectivity (NATs, mobility..)
- draft-hautakorpi-p2psip-with-hip-01.txt (our approach)
  - How HIP (as-is) can be used with P2PSIP
  - Set up P2P and overlay connections using HIP
    - Use the (application-layer) overlay to locate RVS, relays and to route the BEX
  - To be used in together with a P2PSIP protocol proposial

The prototype

- Developed at HIIT as a tool for research in P2P security
  - SPAM/SPIT prevention, privacy issues
- Implemented as a light SIP proxy on Linux
  - HIPL used for HIP
  - Proxy @ localhost, used through normal, unmodified SIP UAs
    - SIP UA (e.g. ekiga, gaim, wengophone) need not be HIP-aware (or even ipv6 enabled!)
- Overlay is separated into distributed storage & routing
  - Multiple simultaneous storage modules possible (DHT-based or not, with or without HIP)
  - Differs from the draft's model

The prototype

- The P2PSIP proxy intercepts SIP messages
  - Converts to P2P format & activities
  - Sets up HIP connections, directs the application to use them (replaces contact addresses with HITs in SIP signalling)



Identity – locator mapping

- Uses SIP AOR (sip:bob@example.com) as identities
  - SIP AOR provides mobility in-between sessions (changing device), HIT mobility during session
  - Distributed storage used for SIP AOR -> HIT & locator (+ possible RVS) mapping
- Certificate scheme used to prove identity
  - Identities are issued by authorities
  - Multiple issuers possible (and recommended!), e.g. company-internal, global, between friends
- SSH-like leap of faith also supported

Next steps

- Routing BEX through the overlay
  - Use the overlay(s) as distributed RVS
  - Like Hi3, but for other overlays as well
- Implementation issues
  - New interface / API in HIPL needed for exporting / importing HIP packets (“alternative transport”)
  - Data formats, encoding (encapsulation) of HIP messages in overlays

Next steps

- Peers can be reached through multiple channels
  - Through RVS, overlay or ipv4/6 directly (possible traversing NATs)
- To minimize connection establishment delay, we would like to try these channels in parallel
- Implementation issues
  - More agile HIP connection establishment interface

Demo

- Deployment
- Creating & importing an identity
- Contacting peer