HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

A secure P2P SIP system with SPAM prevention

Joakim Koskela, Juho Heikkilä, Andrei Gurtov

joakim.koskela@hiit.fi, juho.heikkila@hiit.fi, andrei.gurtov@hiit.fi

http://trustinet.hiit.fi

Motivation

- The security in the emerging, open, P2P systems cannot be based on the same assumptions as in centralized systems
- By incorporating security into the design, we prevent infestation by nuisances, such as SPAM, and security threats

Background

- Currently the IETF is working on a peer-to-peer equivalent of the Session Initiation Protocol (SIP) for serverless and ad-hoc deployments
- The Host Identity Protocol (HIP) is a protocol for identifier/locator split based on crypto-graphically generated identities
- Social networks can be used to model trust relations between people

The Trustworthy Internet -project

- The P2P SIP system, part of the Trustworthy Internet project at HIIT, experiments with models and methods for creating more secure distributed communication systems, such as SPAM prevention in P2P networks

Architecture

- Linux-based P2PSIP prototype uses HIP for all P2P media connections, as it provides strong security, NAT traversal, mobility and multi-homing without additional development efforts
- The identities and integrity of the system is based on public keys and certification by trusted third parties
- The prototype can use any storage system offering a hashtable-like interface for peer lookup, whether distributed or centralized, trusted or untrusted
- The pathfinder provides a privacy preserving way of perceiving the social network beyond first hop
- Pathfinders can be launched as stand-alone HTTP servers. While they do not need the overlay to operate, it can be used to locate them as any other node.

Performance

- The system is currently used in a small-scale trial on hand-held Nokia N810 Internet tablets
- Although the initial HIP base-exchange adds a noticeable delay to the connection set-up, the performance of the tablets is sufficient to secure and manage the mobility of voice and video calls
- The pathfinder delay varies related to the traversed nodes. Callers who are socially distant are more prone to suffer from delays.

Future work

- The design and utilization of HIP-based overlays
- Usability studies through trials and interviews, identifying problems and improvements for the user interface
- Use of descriptive metadata and weights to trust links to provide more accurate estimates and path descriptions

Pathfinder

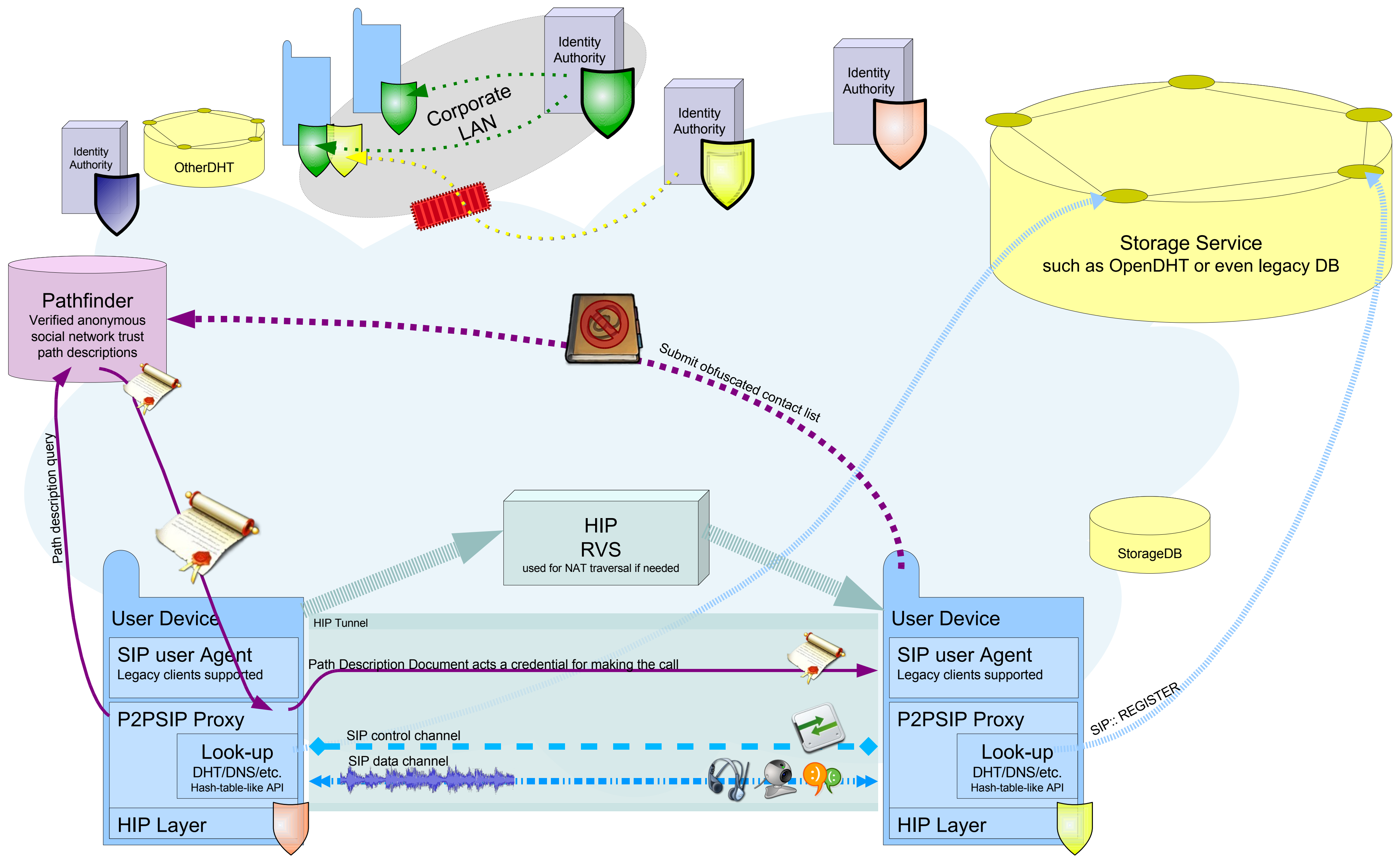
- To filter out calls coming from outside social neighborhood, the recipient proxy needs to know the relative position of the caller
- Users should not disclose their contact lists to the general public, so a trusted third party is needed
- The pathfinder maintains a privacy protected database of social trust links between users and provides path description statements which can be used as credentials for passing the call

Identity Authority

- The SIP identities are tied to public keys by trusted third-party issued certificates. These third-party identity issuers, identity authorities, ensure the uniqueness of each identity
- After the identity has been acquired, no further contact with the identity authority is required
- Multiple authorities are possible, with users trusting, and even having identities issued by more than one

Storage

- Users need to acquire information on the current state of peers, including location and RVS registrations, to establish HIP tunnels
- For the lookup service of this registration information, the system can use any storage service offering a hash-table like interface
- The integrity of the data is verified by the peers, making use of untrusted storage services possible
- Current implementation supports ad-hoc broad-cast, OpenDHT and a web-based storage service



HIP

- The Host Identity Protocol implements the identifier/locator split and secures the peer connections using cryptographically generated identities, DoS protection and encryption of the data traffic
- HIP offers also mobility, NAT-traversal and multihoming with no additional effort for the application development

Software Architecture

- The prototype is implemented as a SIP proxy on Linux, with few library dependencies, allowing it to be run on resource-limited mobile devices
- As a SIP proxy, existing SIP VoIP applications are used unmodified as the user interface
- HIIT's *HIP for Linux* (HIPL)[1] stack is used to provide HIP connectivity.

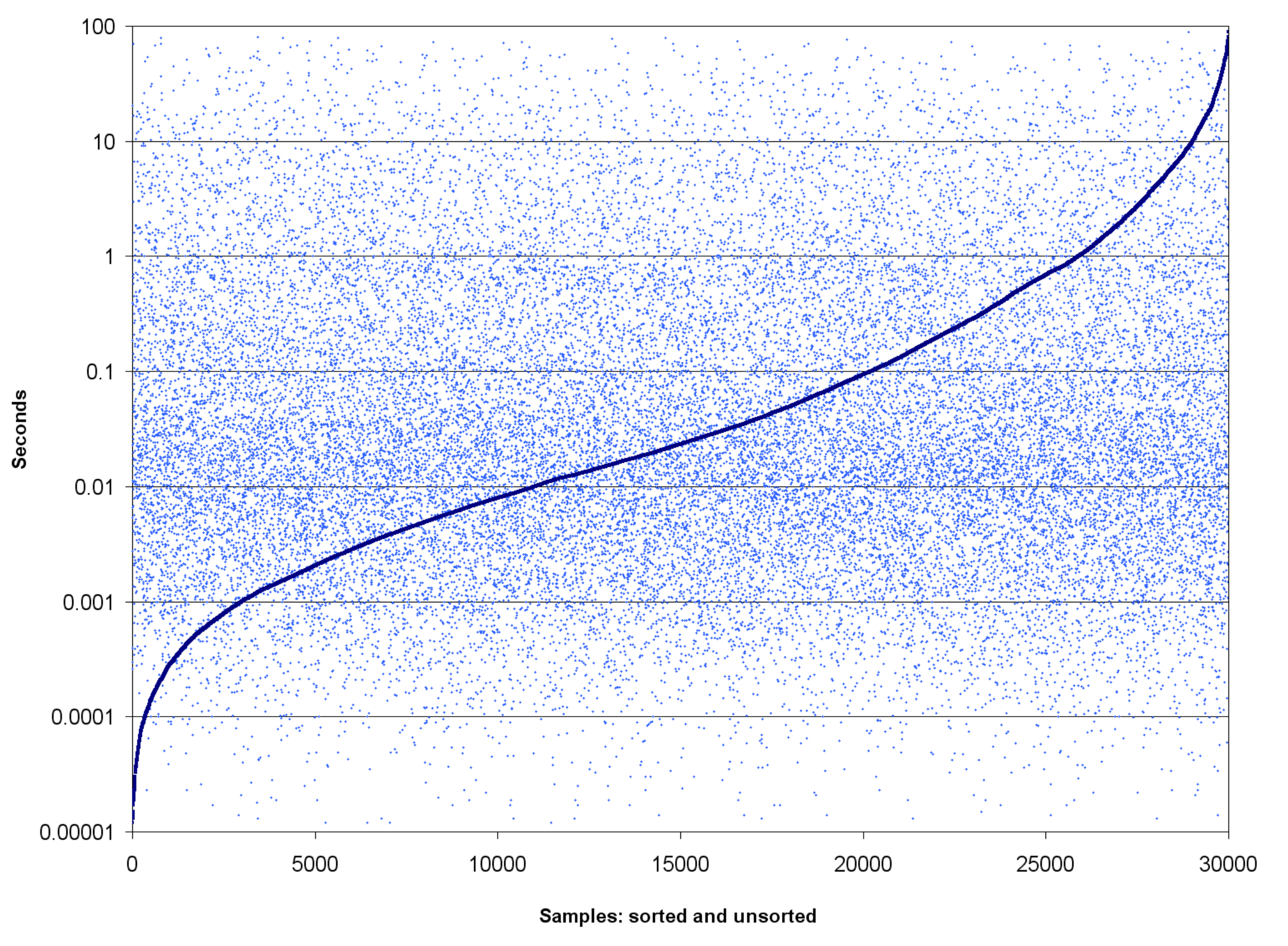
[1] Available at http://hipl.hiit.fi

Tunnel

- Peer connections are established using HIP. The HIP stack handles possible NAT traversal and any mobility updates that might occur
- Within the HIP tunnels, the peers exchange SIP signaling, trust credentials and other data required by the P2P protocol
- The application data, such as voice and video data, is also protected by the HIP tunnel

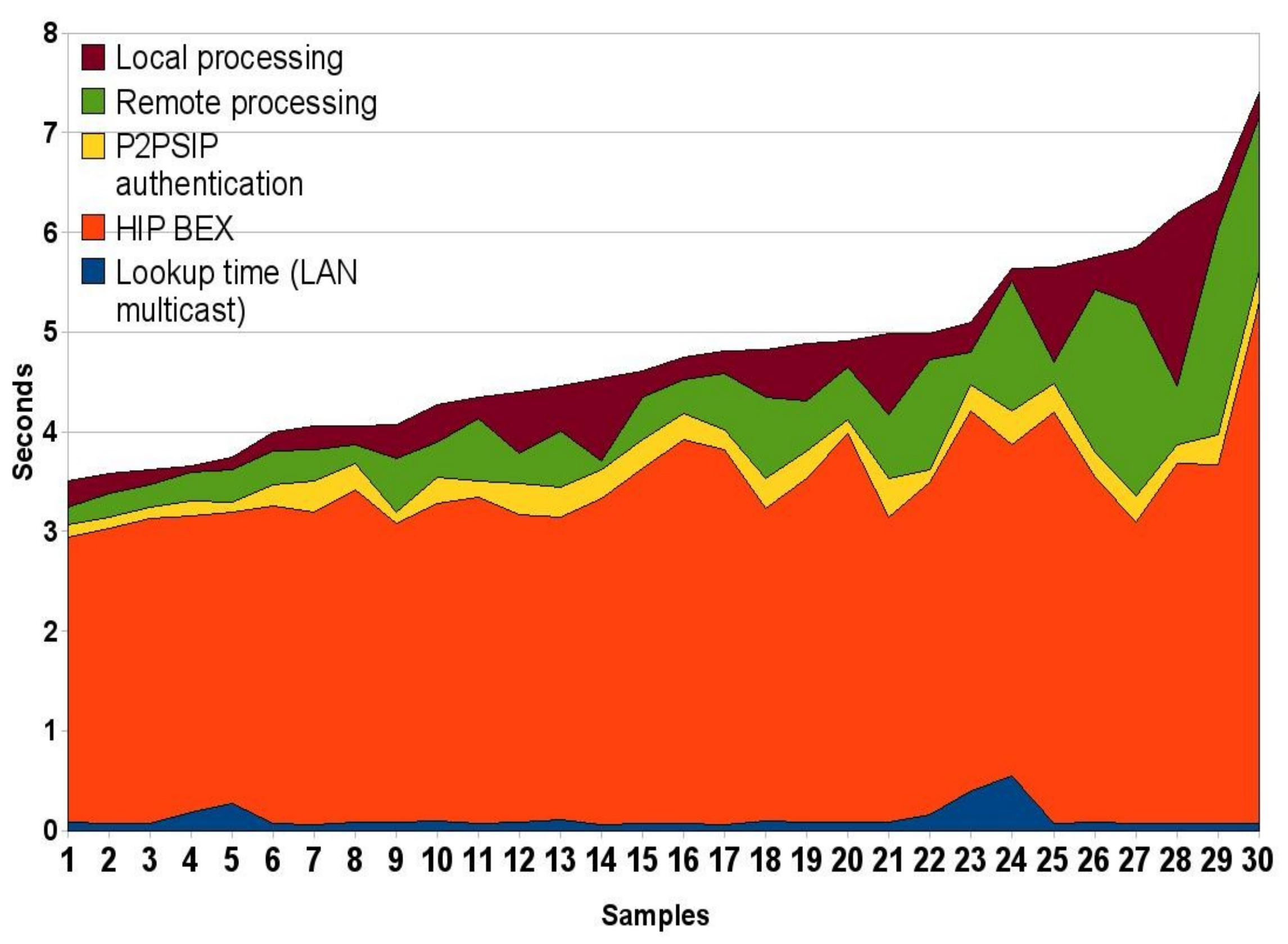
Private networks and LANs

- As the system is not dependent on any global or centralized entity, private and ad-hoc deployments are possible
- The identity scheme allows users to take part in both private communities, such as company intranets, as well as public, global ones



Pathfinder Performance

- We tested the performance of the pathfinding algorithm by making 30 000 random-to-random searches in a social network of 35000 nodes, namely the PGP Web of Trust.
- The figure presents results in measurement order unsorted (cloud) as well as sorted by time (curve)
- The maximum path length was set to 6 hops
- Median result: 23 ms, maximum 104 s.
- The tests were ran on an Athlon XP 3500+ single core PC



Call Delay Measurements

- Post-Dial Delay (PDD) is the interval between completing dialing and receiving a dial tone and is used to express efficiency of telephone systems.
- The measurements were made using two HIP-enabled Nokia N810 Internet tablets (TI OMAP2420 400 MHz CPU, 128 Mb DDR RAM) in 802.11b and g wireless networks using LAN broadcast lookup
- The HIP base-exchange adds a significant delay to the PDD on the tablets. The use of a HIP-secured data tunnel had no noticeable effect on the voice- and video data in terms of delay or jitter

HIIT is a joint research institution of Helsinki University of Technology (TKK) and the University of Helsinki (UH).