Service-Aware Transport Overlays
Ambient Networks Phase 2 – WP-F

https://datatracker.ietf.org/drafts/draft-stiemerling-p2psip-impl/

Martin Stiemerling
<stiemerling@netlab.nec.de>
NEC Laboratories Europe – Network Division
Heidelberg, Germany
Overall SATO Concepts

- **Providing flexible and customisable transport services** to the application layer by using an overlay network on top of basic AN connectivity;

- **Dynamic inclusion of network elements** – the so-called overlay nodes – in the end-to-end transport path. Overlay nodes can provide value added functions such as media adaptation, routing, caching, rate adaptation, synchronization, filtering, metering, congestion control, etc.

- **An Ambient Service Interface (ASI)** that on the one hand hides underlying transport complexity from applications/services, but on the other hand allows applications/services to intelligently customise the transport services to their particular needs.

- **Adaptability of the overlay networks**: overlay networks and overlay nodes are dynamically reconfigured to adapt to changing conditions like, network context, QoS, mobility, and network composition.

- **Automatic management**: self-configuration, self-healing, self-protection, self-securing, self-optimisation, self activation of overlay networks:

- **Reliability and resilience**: fault-tolerant protocols, algorithms and state stores that survive failures/removal of overlay nodes and overlay control nodes without loosing the control and state of configured overlays.

- **Optimised cross layer performance** between the transport overlay layer and the underlying network connectivity layer.

- **Charging and metering**: capabilities for metering in overlay nodes and charging of transport services.

- **Secure overlays**: secure overlay networks can be used to protect from e.g. DoS attacks.
SATO in a Nutshell

• Provide generic overlay system for applications, e.g.,
  – IPTV
  – Peer-to-Peer SIP
• Provide flexible and customizable Overlay Network layer
  – Service-aware Transport Overlay (SATO)
  – Dynamic inclusion of network processing elements (SATO Ports)
  – On-demand Overlay per service set up and tear down
  – Dynamic adaptation to changes (network, context, etc.)
• Service paths composed by Overlay Nodes (ONodes)
  – SATO controller (Overlay Manager)
  – Hosting one or more SATO Ports (SPs)
  – Additional elements for communication, resources mngt, etc.
• Generalized lookup service
  – API to (distributed database)
  – Currently using a database and a DHT for testing
SATO Network Architecture

Media Applications / Services

Ambient Service Interface

ACS

Transport Overlay Control

Mobility

Security

Context Information

Control

Data

Overlay Node

Router

Terminal/Host

SSON 1

- Metering
- Caching
- Media Adaptation
- etc.

- Client
- Server
Ambient Networks System Interfaces

Application

ASI Interface

SATO

Socket Interfaces

NodeID

IPv4/IPv6

Ambient Network Interface (ANI)

Application

SATO

NodeID

IPv4/IPv6
SATO Node Architecture

SATO Data Plane Interface

Processing
SATO-Port

Functions
SATO-Port

Overlay Management

Lookup-Service (e.g. DHT)

NodeID/IPv4/IPv6 network stack

SATO Control Plane Interface

OM IF

DHT IF
HIP and SATO

• SATO network requirements
  – Actually none, i.e., take what you have ;-)  
  – E.g., IPv4, IPv6, ID/Locator split
• SATO is aiming at enhancing network layer (among others)
  – Hide IPv4/IPv6
  – Add authentication and crypto
  – Sounds like ID/Loc Split and HIP...
• SATO actually uses HIP++ = NodeID
  – Simon’s talk at HIPRG@IETF#68 and RRG@IETF#70
• NodeID features in a nutshell
  – Currently NodeID = HostID of HIP  
  – Crypto. ID
  – NodeID is used for routing IP packets
  – NodeID introduces NAT-PT to bridge IPv4 and IPv6
  – NodeID also allows IPv4 host to directly communicate with IPv6 hosts
• NodeID used
  – in P2PSIP URI to “address” mapping
  – To setup overlay links between nodes (virtual link)
  – NodeID ensures NID-aware NAT traversal
  – SATO takes care about NID unaware NATs
  – Ensure that the nodes you’re talking to are the ones you want to
NodeID Architecture

Bearer with various characteristics

Path selection

End-to-end security is based on NIDs.

Domains are connected by “NID routers” that route based on destination NIDs

Identifier Name Space

Locator domains have independent address spaces

Self-configuration of base connectivity

Mapping/binding

Nodes have Node IDs, self-generated public keys

End-to-end security is based on NIDs.

Bearer with various characteristics

Path selection

Domains are connected by “NID routers” that route based on destination NIDs

Identifier Name Space

Locator domains have independent address spaces

Self-configuration of base connectivity

Mapping/binding

Nodes have Node IDs, self-generated public keys
P2PSIP as SATO Usage Example
P2P Overlay Adaptation

P2P NW

SATO Port

Overlay (tunnel)

SIP

Overlay (tunnel)

RTP

Internet

SATO Port

RTP

SIP

RTP
P2P Overlay Adaptation

P2P NW

SATO Port

SIP

Overlay (tunnel)

RTP

SATO Port

SIP

Overlay (tunnel)

RTP

Internet
P2P Overlay Adaptation

SATO

P2P NW

Overlay (tunnel)

SIP

SATO Port

Internet

SIP

RTP

RTP
Conclusions

- SATO system specification is almost complete
- Background algorithms are partially missing
  - e.g., creation of SATOPort chains for complex services
- Prototype implementation ready
  - Two types: IPTV and P2PSIP
- Open issues
  - Automatic management
  - Reliability and resilience
  - Optimised cross layer performance
  - Consists and long-time usable naming and addressing
  - Finding the right SATOPort at the right position
  - Disconnected operation
  - Scalability of system
  - Naming and addressing (cf. ID/Locator split discussions)
Empowered by Innovation

NEC