



# End-to-end mobility solutions

**(A comparison of non-MIP ways of Internet mobility)**

Falko Hansen-Hogrefe

Email: [studium@hansen-hogrefe.de](mailto:studium@hansen-hogrefe.de)

Telematics Group  
Institute for Informatics  
University of Göttingen, Germany



# Table of contents

- Introduction
  - Mobile IP
- An end-to-end approach to host mobility (A. C. Snoeren and H. Balakrishnan)
  - basic principles
  - connection migration
  - evaluation
- Integrating Security, Mobility, and Multi-homing in a HIP Way (P. Nikander, J. Ylitalo, and J. Wall)
  - overview
  - requirements
  - implementation status

# Table of contents (cont.)

- A new Scheme for IP-based Internet-Mobility
  - (T. Dreibhoz, A. Jungmaier, M. Tüxen)
  - Stream Control Transmission Protocol (SCTP)
    - Mobile SCTP
  - Reliable Server Pooling
  - results
- comparison
- conclusion

# Introduction

- Mobile IP
  - current standard for internet mobility support
    - creates routing tunnel between mobile host and it's home agent
  - problems
    - causes triangular routing without optimization
    - optimisation requires modifications to infrastructure and IP layer at end hosts

# An end to end approach to host mobility

- uses **DomainNameSystem for location updates**
  - **client: normal DNS, new query when server moved**
  - **server: has to perform a dynamic DNS update**
- **TCP connection migration**
  - **Id: 4tuple (source IP – Port ; destination IP – Port)**
  - **other identifier required when IP-Port changes**
    - **replaced by a token to recover the connection**
    - **also secures the connection as key (Elliptic Curve**

# Connection Migration

- new TCP option allows IP address change on established connections
  - extends SYN packet with migration option
  - token computed during connection establishment
  - when a host changes send SYN with
    - token to recognise and recover connection
    - a request
    - sequence number prevents reordering
  - compare token to identify connection
  - ACK to new IP-Port pair from last SYN

# Connection Migration (ext. SYN)

- migrateable connection initiation
  - secure Length=20 containing key
  - insecure Length=3 keys set to zero
- migrate option
- contained in SYN
  - to migrate a connection
  - instead of “normal” initiation

Kind: 15	Length = 3/20	Curve Name	ECDH PK
ECDH Public Key (cont.)			
ECDH Public Key (cont.)			
ECDH Public Key (cont.)			
ECDH Public Key (cont.)			

	Kind: 16	Length = 19	ReqNo
Token			
Token (cont.)			
Request			
Request (cont.)			

# Evaluation

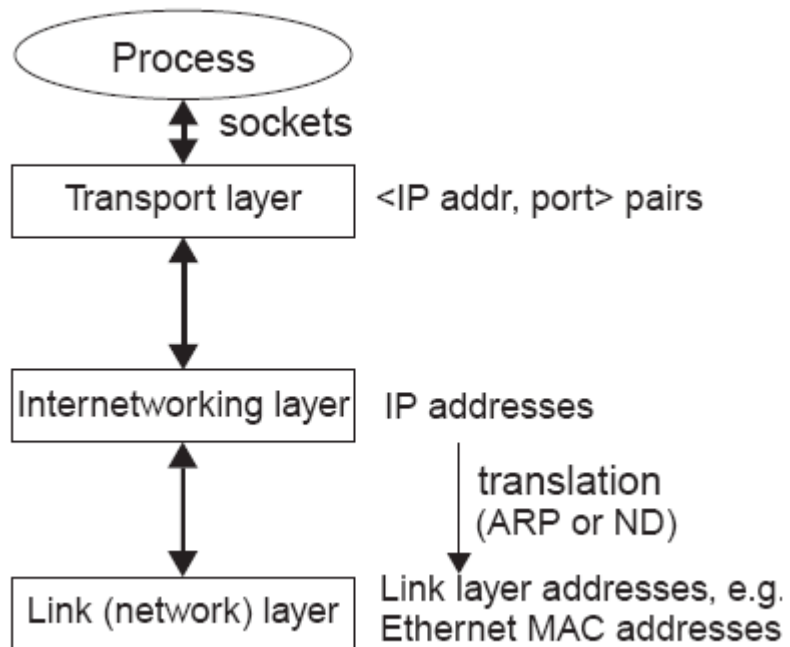
- each transport protocol has to be extended with the connection migration option
  - TCP implementation generalisable to other specific UDP-based protocols (e.g. Real-time Transport Protocol)
  - other often already have control messages that may be easily extended
- not all applications need mobility support
- no changes to IP structure or routers

# Integrating Security, Mobility and Multi-homing in a HIP way

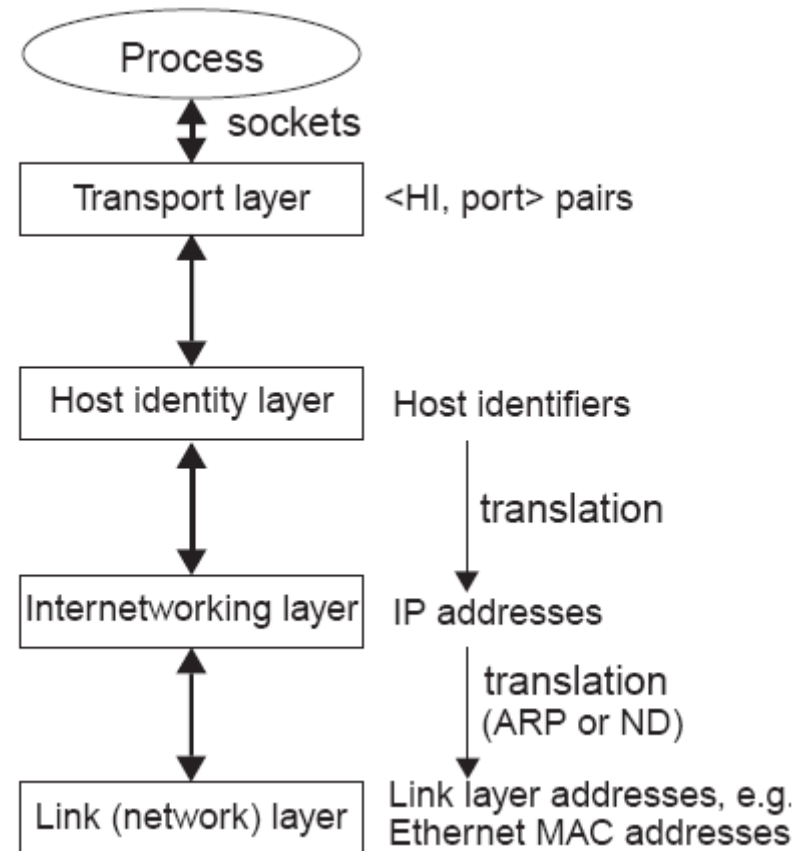
- IP address today represents the hosts identity **and** location
  - hence a new location (mobility) also changes identity
  - several IP addresses possible (e.g. wlan and GPRS) but no switch from one to another (due to better link quality or costs)
  - this prevents mobility and multi-homing support
- idea is to separate identity and location
  - IP keeps representation of the location (potentially multiple)
  - Host Identifiers (HI) represent end points without location binding

# New layer structure

## current architecture



## proposed



# Requirements for new architecture

- Host identifier
  - represented by public part of a key pair to identify the end-point
  - More than one possible to e.g. protect privacy
- Address Discovery Service
  - similar to DNS it resolves HI  $\leftrightarrow$  IP resolution but a **set of addresses not only single one**
  - **protocols to query the service**
- **possibility to inform corresponding hosts about changes**

# Requirements (cont.)

- **Security**
  - **no more authentication by infrastructure on the base of IP**
  - **explicit one needed to prevent**
    - **address stealing**
    - **flooding attacks**
  - **authentication with a public key (identical to HI) so no public key infrastructure is needed**

# Implementation status and further work

- test implementation HLP/HIP for NetBSD 1.6
- basic implementation seems to be easy realisable
- cleaning up expired HI  $\leftrightarrow$  IP bindings and performance optimization seems to require extensive modifications to the kernel and TCP algorithms
  - the authors expect that other projects e.g. SCTP faced this problems

# A new scheme for IP-based Internet-Mobility

- based on reliable **Stream Control Transmission Protocol with enhanced with dynamic address reconfiguration (Mobile SCTP)**
  - provides persistent connections if only one host moves at the same time
- additional uses **Reliable Server Pooling based protocol**
  - to cover weak spot of **SCTP: simultaneously host movement**

# Stream Control Transmission Protocol

- SCTP packet format
  - header
    - similar to TCP and UDP
    - tag (randomly chosen to secure the association)
    - checksum
  - chunks containing
    - data
    - control messages
- supports Multi-Homing Dynamic Address Reconfiguration (control chunks)

# Mobile SCTP

- Mobile Hosts monitor the network attachment of their interfaces
  - new or no longer available connections are announced to peers with ASCONF (Address Configuration)
- allows no simultaneously movement of both linked hosts possible
  - solutions
    - Mobile IP(v6)
    - dynDNS
    - RSerPool

# Reliable Server Pooling

- uses redundant nodes (server pools)
  - improves reliability (no single point of failure)
  - flat name space allows any pool ID (e.g. ASCII string)
  - nodes can (re)register as pool members at nameservers (NSs)
- NSs manage and control paths to pool servers
  - unreachable servers are removed
    - unanswered keep alives from NS
    - client reports unreachable server to NS
- NS announces subset of all pool members
  - client chooses one from given subset

## Results

- test implementation shows that this approach fits the mobility requirements
  - failed connection recognition should be optimized to minimize time of no data transfer
- for today's situation (especially clients are mobile) Mobile SCTP is sufficient
- with RSePool it may fit all mobility scenarios
- to optimise parameter settings on (mobile)SCTP for performance improvements
  - simulations with OPNET are planed

# Comparison

	<b>Mobile IP</b>	<b>dynDNS</b>	<b>HIP</b>	<b>SCTP</b>
modified layer	network	transport & application	new one between transport&network	transport (RSerPool: session)
additional needs or changes	IP-layer & routing infrastructure	additional TCP option & Field in TCB	Host Identify Layer	mobile extension to SCTP
security	extra protocol implemented	dynDNS features & token	public key without infrastructure needs	tag (cookie) identifies association

# Conclusion

- all approaches uses same idea of announcing new point of attachment to corresponding hosts
  - direct
    - via additional control messages
    - big problem simultaneously moving hosts
  - indirect
    - needs a non moving representative
    - can solve the problem of simultaneous movement
- in addition to mobile IP these approaches care of multi-homing and some additional security

## Conclusion (cont.)

- research in this field is still in progress
  - only early test implementations
  - not clear if suitable for daily use
- often problems are solved falling back on parts from other solutions
  - maybe combining the solutions will lead to better results or give new ideas
- which one will be the leading part in the future is incalculable

thank you for your attention