End-to-end mobility solutions

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

Falko Hansen-Hogrefe
Email: 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
  – 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
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 its 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 Diffie-Hellman)
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

<table>
<thead>
<tr>
<th>Kind</th>
<th>Length</th>
<th>Curve Name</th>
<th>ECDH PK</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>3/20</td>
<td></td>
<td>ECDH Public Key (cont.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ECDH Public Key (cont.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ECDH Public Key (cont.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ECDH Public Key (cont.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kind</th>
<th>Length</th>
<th>ReqNo</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Token</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Token (cont.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Request (cont.)</td>
</tr>
</tbody>
</table>
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 host's 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 architecture

- Process
  - Sockets
  - Transport layer
    - <IP addr, port> pairs
  - Internetworking layer
    - IP addresses
      - Translation (ARP or ND)
  - Link (network) layer
    - Link layer addresses, e.g. Ethernet MAC addresses

- Host identity layer
  - Host identifiers
    - Translation
  - Internetworking layer
    - IP addresses
  - Link (network) layer
    - Link layer addresses, e.g. Ethernet MAC addresses
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 <-> 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 <-> 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 massages

- 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 planned
### Comparison

<table>
<thead>
<tr>
<th>Modified layer</th>
<th>Mobile IP</th>
<th>dynDNS</th>
<th>HIP</th>
<th>SCTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP-layer &amp; routing infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>extra protocol implemented</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP-layer &amp; routing infrastructure</td>
<td>transport &amp; application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>extra protocol implemented</td>
<td>additional TCP option &amp; Field in TCB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>transport &amp; application</td>
<td>dynDNS features &amp; token</td>
<td></td>
<td>new one between transport &amp; network</td>
<td>mobile extent ion to SCTP</td>
</tr>
<tr>
<td>added TCP option &amp; Field in TCB</td>
<td>Host Identify Layer</td>
<td></td>
<td></td>
<td>tag (cookie) identifies association</td>
</tr>
<tr>
<td>new one between transport &amp; network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>new one between transport &amp; network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

• all approaches use the same idea of announcing a 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 for 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