Fast, Secure Failover for IP

Saleem Bhatti
& Ditchaphong Phoomikiatissak
University of St Andrews, UK

Ran Atkinson
Cheltenham Research, USA

http://ilnp.cs.st-andrews.ac.uk/

S. N. Bhatti, D. Phoomikiatissak, and R. Atkinson,
"Fast, Secure Failover for IP",
IEEE MILCOM 2014, 08 Oct 2014

Outline

- Problem space
- Introduction to ILNP
- IPsec failover solution using ILNP:
  - architecture
  - evaluation
- Summary
- Questions

Problem space

Graceful failover for IPsec

- **IPsec graceful failover currently not defined:**
  - no standard mechanism
  - proprietary solutions exist
  - (IPsec is the basis for military HAIPE IP encryptors)
- Graceful:
  - IPsec session should not be interrupted
  - interruption of IPsec traffic should be minimal
  - failover should be invisible to end-systems

IPsec today

- IPsec Security Association (SA) binds to an IP address:
  - IP address has topological semantics
  - IP address is used as a form of identity
- Failover:
  - connectivity change may involve change of IP address range (new IP routing prefix)
  - change in IP prefix changes end-system state for IPsec (and also for upper layer protocols, e.g. TCP)

End system state for an IP session

- Example: end-system state in TCP/IP
- IP addresses, A
- Transport-layer Port numbers, P
- Changes to interface address binding has impact higher up the stack

$$\langle tcp : P_X, P_Y, A_X, A_Y \rangle \langle ip : A_X, A_Y \rangle \langle i/f : A_X \rangle$$

Current naming architecture

Protocol Layer	IP
Application	FQDN or IP address
Transport	IP address (+ port number)
Network	IP address
(Interface)	IP address

Entanglement ☹

FQDN = fully qualified domain name

Introduction to the Identifier Locator Network Protocol (ILNP)

New naming architecture: IP vs ILNP

Protocol Layer	IP	ILNP
Application	FQDN or IP address	FQDN (RFC1958)
Transport	IP address (+ port number)	(Node) Identifier (+ port number)
Network	IP address	Locator
(Interface)	IP address	(dynamic mapping)
	Entanglement ☹	**Separation ☺**

FQDN = fully qualified domain name

End system state with ILNP

- Example: end-system state in TCP/ILNP:
  - within the context of IPv6
- Locator value, L
- Port numbers, P
- Node Identifier (NID) values, I

$$\langle tcp : P_X, P_Y , I_X, I_Y \rangle \langle ilnp : L_X, L_Y \rangle \langle i/f : (L_X) \rangle$$

$$\langle tcp : P_X, P_Y , A_X, A_Y \rangle \langle ip : A_X, A_Y \rangle \langle i/f : A_X \rangle$$

Locator/Identifier Split for ILNP

- **Locator, L:**
  - **Topologically significant.**
  - Names a (sub)network
  - Similar to today's **network routing prefix**
  - Used only for routing and forwarding in the core.
- **(Node) Identifier, NID:**
  - **Is not topologically significant.**
  - Names a logical/virtual/physical node, does **not** name an interface.
- **Upper layer protocols bind only to Identifier.**

ILNP: Engineering

- Main architectural ideas can be applied as extensions to both IPv4 and IPv6:
  - RFCs 6740-6748 (Experimental, IRTF RRG)
- **ILNP extensions to IPv6 –> ILNPv6.**
- Non-ILNP nodes see an ordinary IPv6 packet.
- ILNPv6 end-systems see an ILNPv6 packet.
- Focus here is on IPv6, as the engineering is cleaner, but IPv4 is also possible.

ILNPv6

- A set of extensions to IPv6:
  - Same packet format as IPv6, with extensions
  - No changes required in the IPv6 routers
  - Incrementally deployable on IPv6 networks
  - Backwards compatible with IPv6 devices
- Split 128-bit IPv6 address:
  - **64-bit Locator (L64) -- (sub)network name.**
  - **64-bit Identifier (NID) -- node name.**

IPv6 addresses and ILNPv6

```
IPv6 (as in RFC3587 + RFC4291):

 | 3 |     45 bits         | 8/16 bits |       64 bits                |
 +---+---------------------+-----------+------------------------------+
 |       Unicast Routing Prefix        |   Interface Identifier       |
 +---+---------------------+-----------+------------------------------+
```

IPv6 routing (address) prefix

same syntax, different semantics

```
ILNPv6:

 |             64 bits                 |       64 bits                |
 +---+---------------------+-----------+------------------------------+
 |             Locator                 |   Node Identifier (NID)      |
 +---+---------------------+-----------+------------------------------+
```

same syntax and semantics as IPv6 routing (address) prefix so IPv6 core routers work as today

these bits only examined and acted upon by end systems

IPv6 packet header

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |   Next Hdr    |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+-                      Source Address                         -+
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+-                    Destination Address                      -+
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ILNPv6 packet header (end-system)

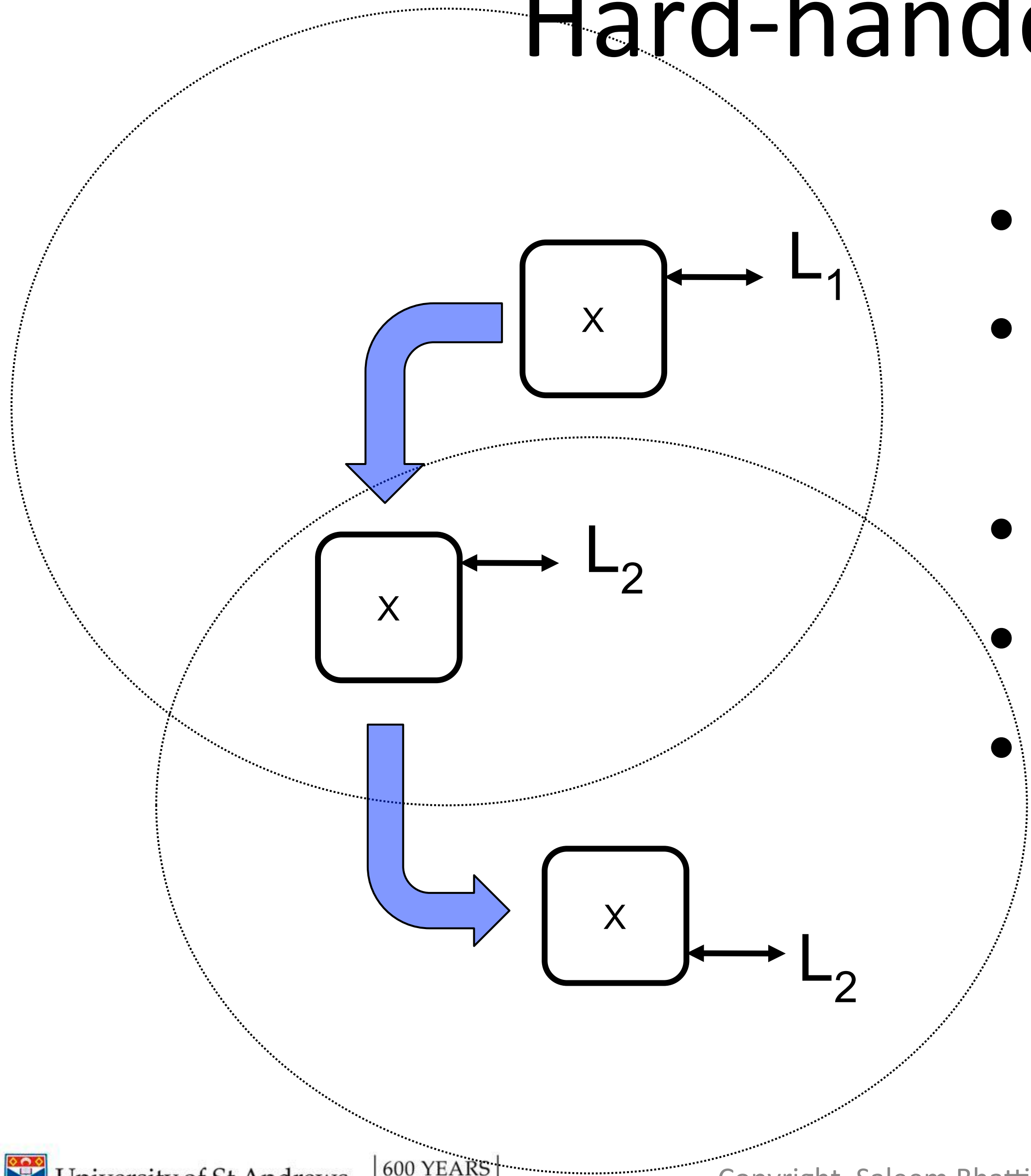
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Hdr     |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Source Locator                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                       Source Identifier                       +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                      Destination Locator                      +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                    Destination Identifier                     +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IPsec failover solution using ILNP

IPsec / HAIPE with ILNP Mobility

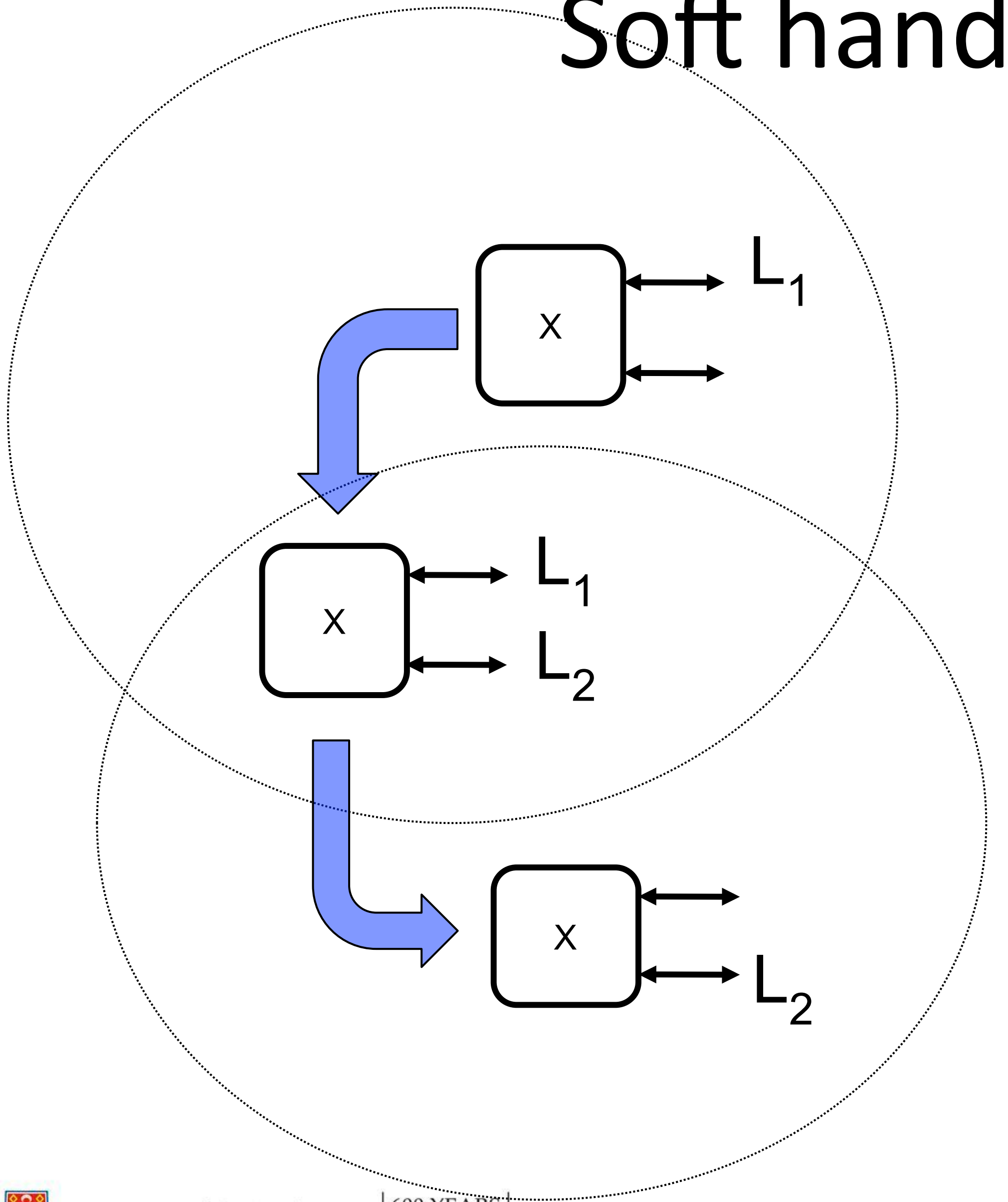
- **IPsec / HAIPE with ILNP binds only to NID:**
  - NID is used in transport layer state
  - NID is not topologically significant
  - preserves end-to-end semantics
- **NID-L binding change does not impact IPsec:**
  - dynamic update of NID-L binding similar to that for Mobile IPv6
  - change in NID-L binding does not impact transport layer sessions
  - Hence, IPsec can be used end-to-end during failover

Hard-handoff [1]



- Start with L_1
- Change IP-level connectivity
- Change L value to L_2
- Use new L_2 value
- Possible packet loss while correspondent node does know about L_2

Soft handoff [1]

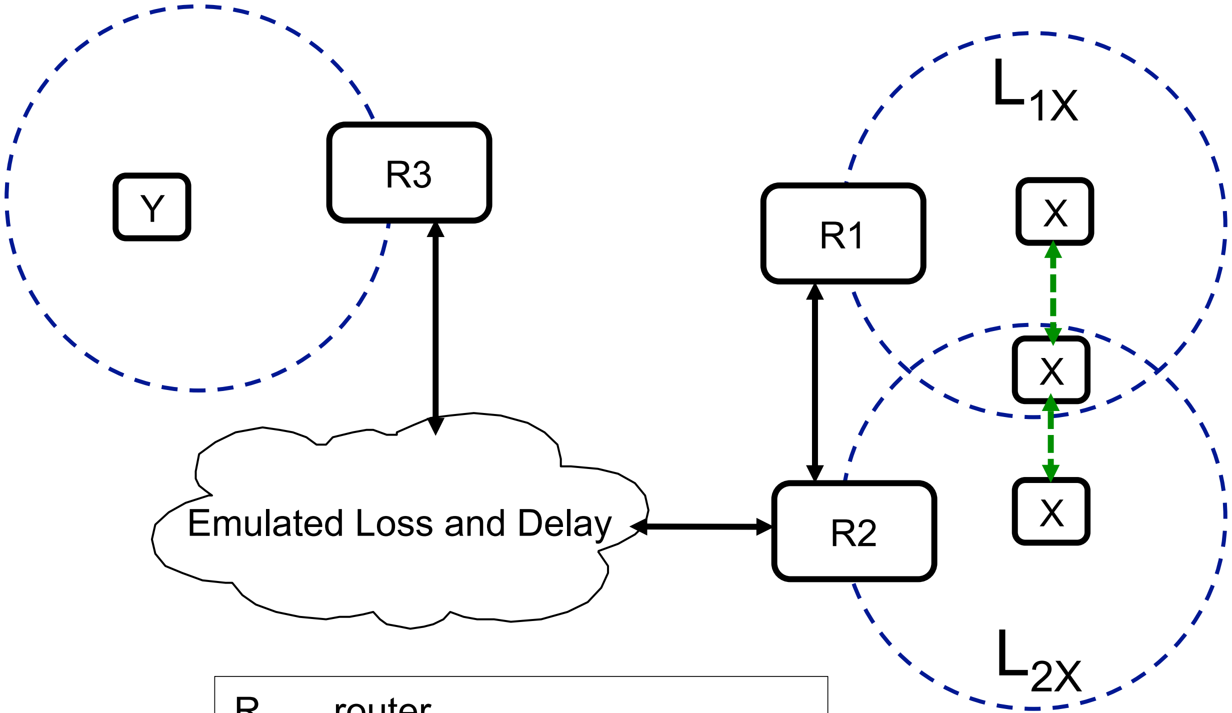


- Start with L_1
- In overlap of cells, use both L_1 and L_2
- Then, handoff to L_2
- Multihoming during handoff
- **Network-layer soft handoff.**

ILNP IPsec advantages

- Completely end-to-end model
- No middleboxes/proxies required – such boxes can be:
  - a single point of failure
  - performance bottleneck
  - point of security attack
- No tunnelling:
  - apart from that which might already be used by IPsec
- No routing changes required:
  - trust boundaries confined to end-systems/sites

Testbed evaluation



R router
L L64 (routing prefix) values
X, Y end-systems

Traffic emulation and metrics

TABLE IV
APPLICATION TRAFFIC EMULATION, FLOWS LASTED 65S.

Description	Data Rate [Kbps]	Pkt Size [bytes]	Ref.
Skype / VoIP	64	300	[55], [56]
YouTube / ViIP	658[a]	1400	[57]

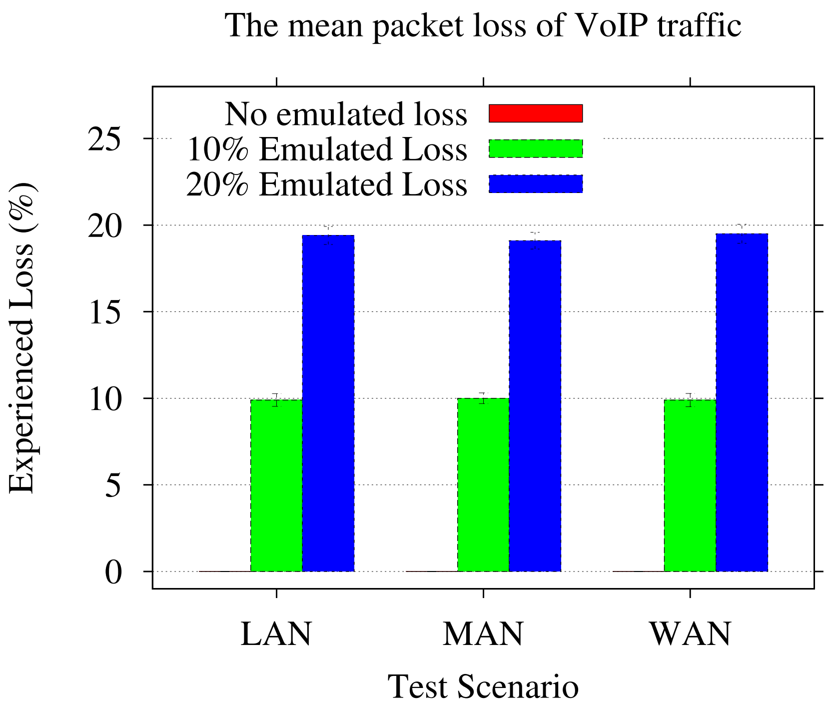
[a] This is slightly more than the 632Kbps reported in [57].

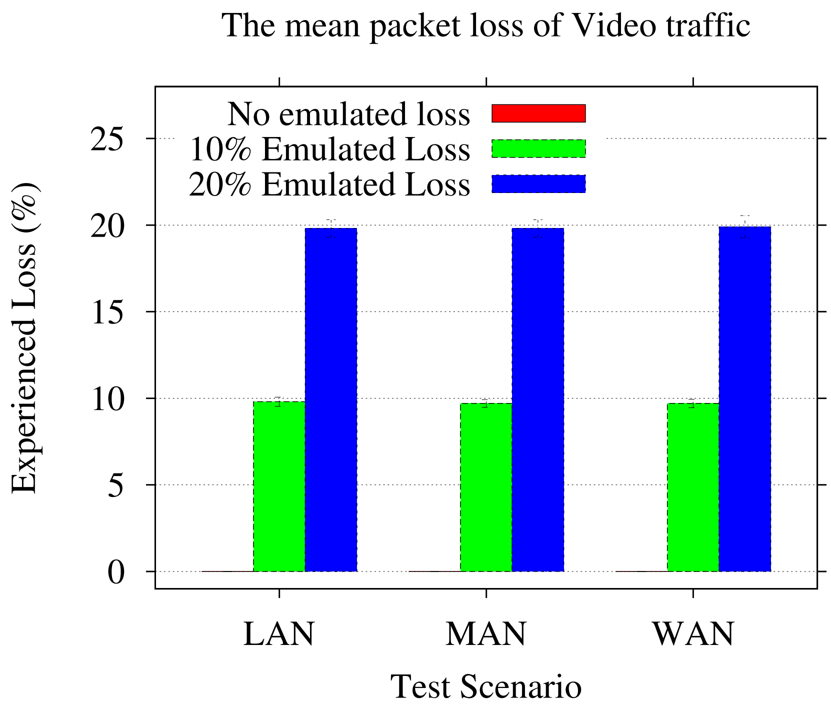
TABLE V
METRICS USED FOR PERFORMANCE EVALUATION.

Metric	Units	Summary	Fig.[a]
loss	%	Application-layer (STP)	4a
f-delay	ms	Time to complete failover	4b
f-overhead	–	# LU/LU-ACK handshakes	4c

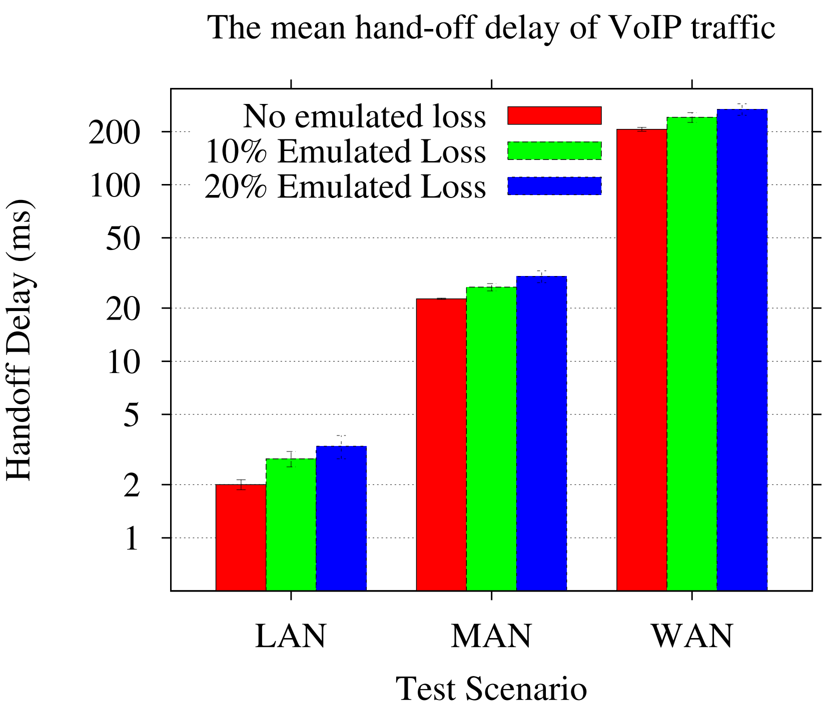
[a] The figure showing the related testbed measurements results.

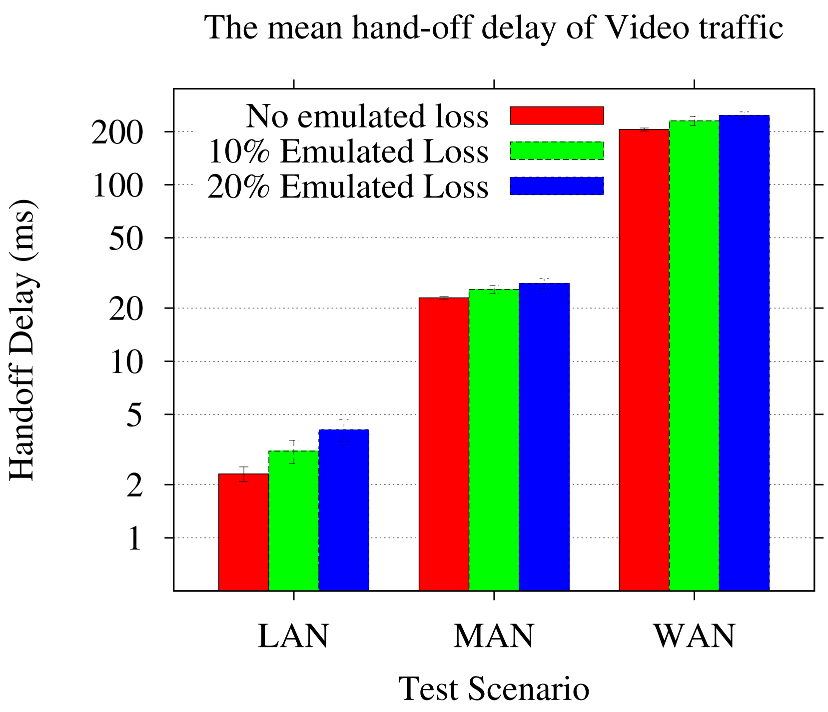
Application layer loss



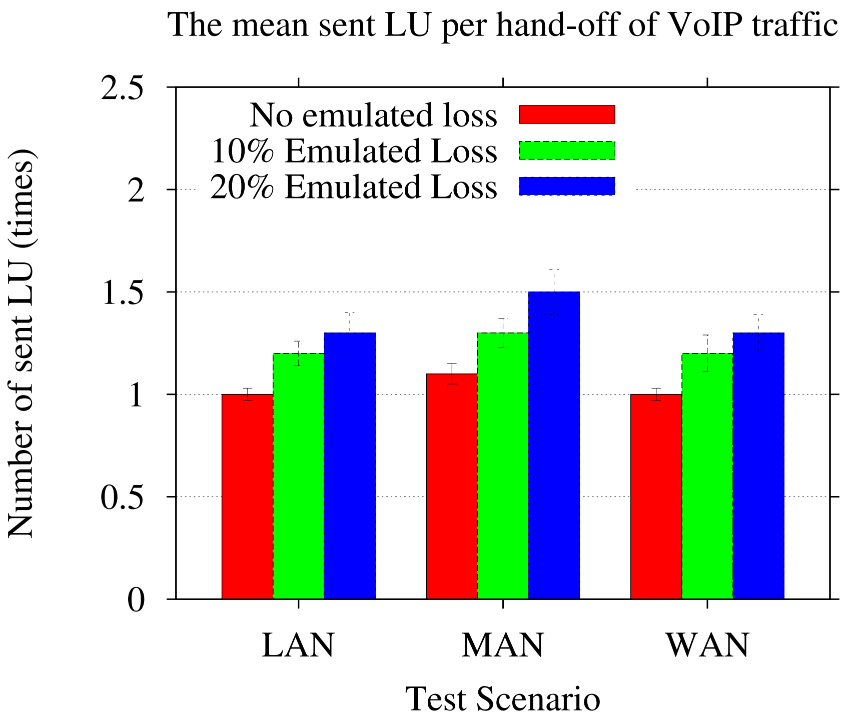


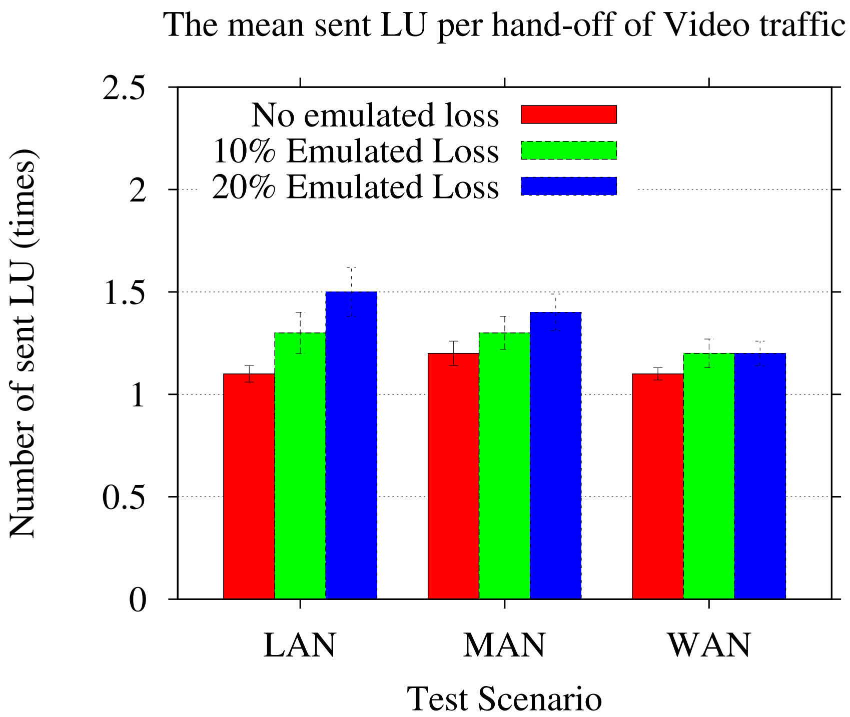
Failover delay





Failover overhead





Summary

ILNP IPsec failover

- IPsec failover with ILNP:
  - mobility model
- End-to-end model - advantages:
  - no proxy/middlebox
  - trust boundary
  - no additional attack vectors via proxy
- Performance:
  - virtually zero gratuitous loss with soft handoff
  - low overhead

Contacts

- Thank you!

- Saleem Bhatti
  - Professor of Computer Science
    University of St Andrews, UK
    saleem@cs.st-andrews.ac.uk
    http://saleem.host.cs.st-andrews.ac.uk/

- Ran Atkinson
  - Independent Consultant
    Cheltenham Research, USA

Backup Slides

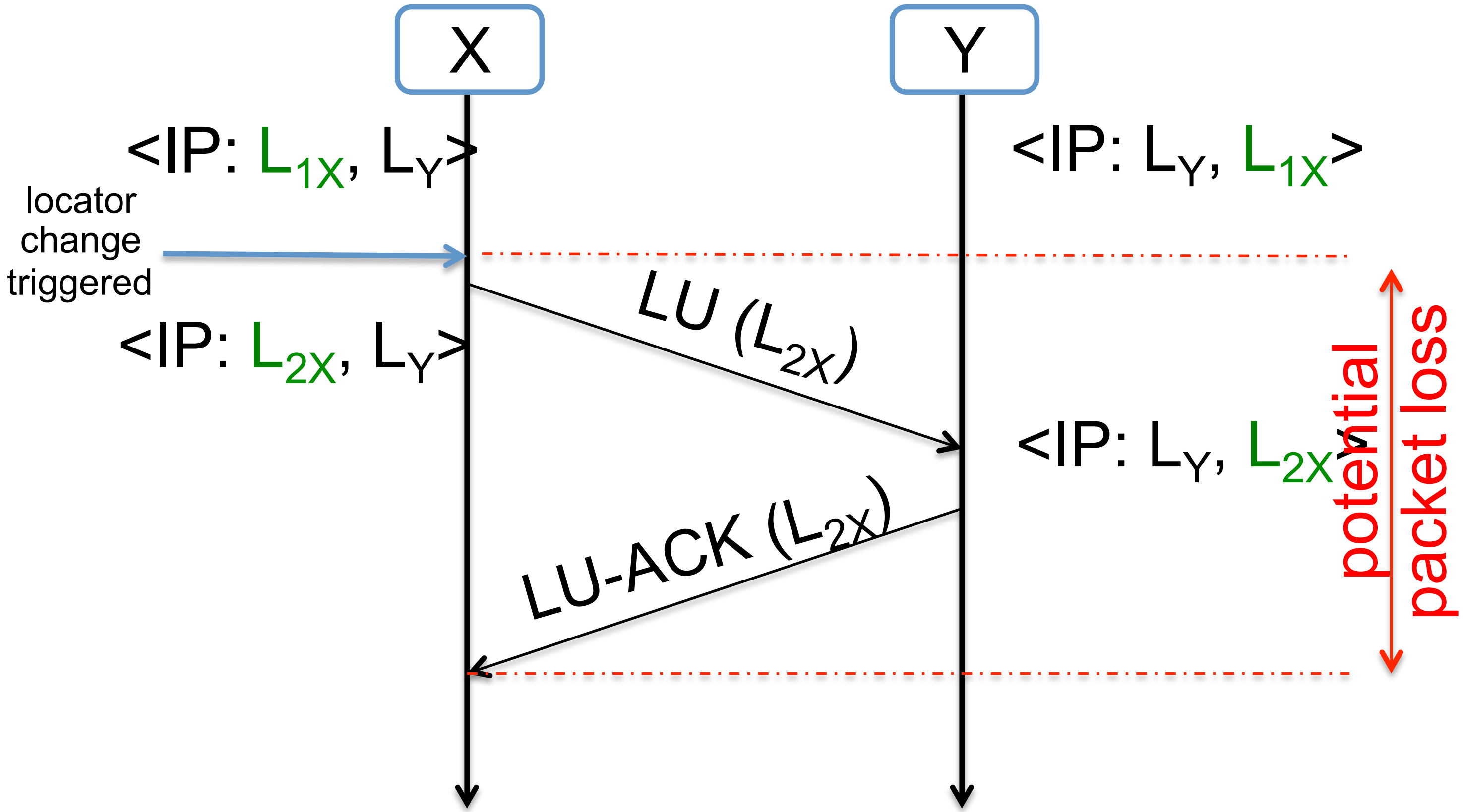
ILNP: Locator Properties

- Locator names an IP Subnetwork.
- Locator is equivalent to an IP Routing Prefix.
- **Nodes can change their Locator values during the lifetime of an ILNP session:**
  - **Enables mobility, multi-homing, NAT, end-to-end IPsec, site-controlled traffic engineering, etc.**
- Multiple Locators can be used simultaneously
  - Enables multi-homing, seamless mobility, end-to-end IPsec, traffic engineering, etc.
- Locators NEVER used by TCP, UDP, SCTP, etc.

ILNP: Identifier Properties

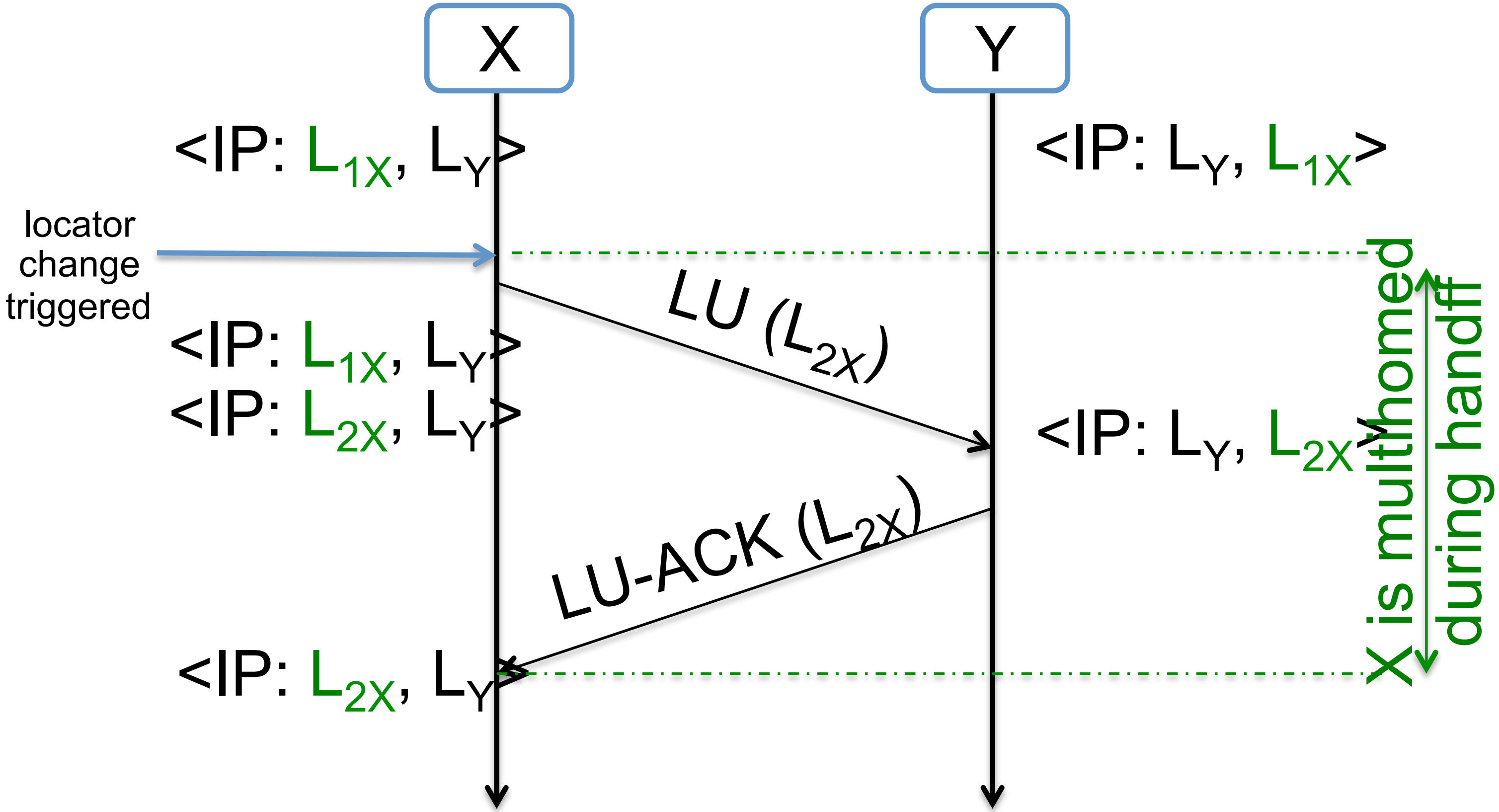
- Identifier names a **node**, not an **interface**
- **Remains constant** during the lifetime of a transport session
  - **Enables IPsec, NAT, & other improvements**
- Nodes have multiple Identifiers concurrently:
  - Only one identifier for a given ILNP session
  - Identifiers are stable over time
- Special NID formats also supported by ILNP:
  - IPv6 Privacy ID extensions, CGAs, etc
- Only NID is used by IPsec, TCP, UDP, SCTP, etc.

Hard-handoff [2]



Hard handoff
(similar to Binding Update for Mobile IPv6)
(new L values can be learned from IPv6 router advertisements)

Soft handoff [2]



Soft handoff

(new L values can be learned from IPv6 router advertisements)