Interoperability and Security of TraSH: A Transport Layer Seamless Handover

Panel Session at

23rd IEEE International Performance, Computing, and Communications Conference

April 16, 2004

Dr. Mohammed Atiquzzaman
University of Oklahoma
Norman, OK 73019-6151, USA.
atiq@ou.edu
www.cs.ou.edu/~atiq

TraSH: Transport layer Seamless Handover

- Basic concepts
  - Decouple location management from handoff
  - Carry out location management and handoff in parallel to data transmission
  - Allow the layer whose performance is to be optimized to take responsibility of the handoff
- Motivation:
  - Performance problems of Mobile IP
  - Design issues of Mobile IP
- Implementation:
  - Multihoming to achieve simultaneous communication with multiple access points.
  - Stream Control Transmission Protocol (RFC 2960).

"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

SCTP: A new Transport Protocol for Internet

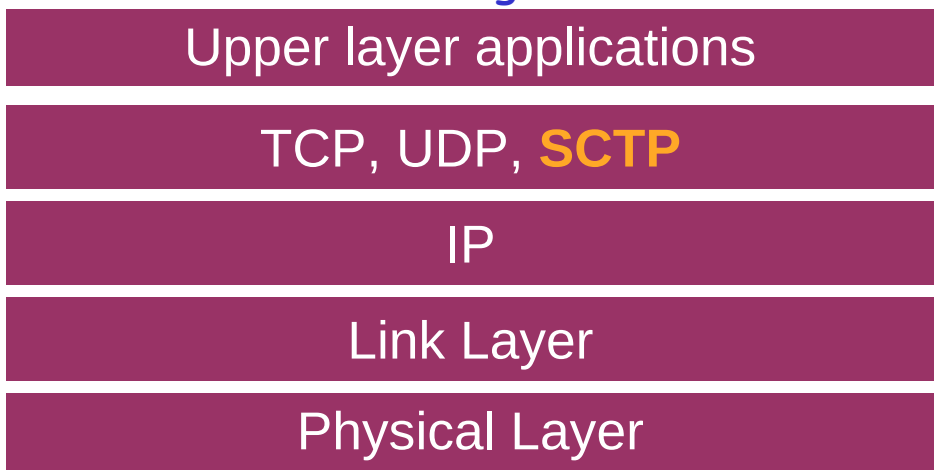
What is SCTP?

- SCTP: "Stream Control Transmission Protocol"
- Originally designed to support SS7 signaling messages over IP networks. Currently supports most of the features of TCP
- Standardized by IETF RFC 2960
- Reliable transport protocol on top of IP

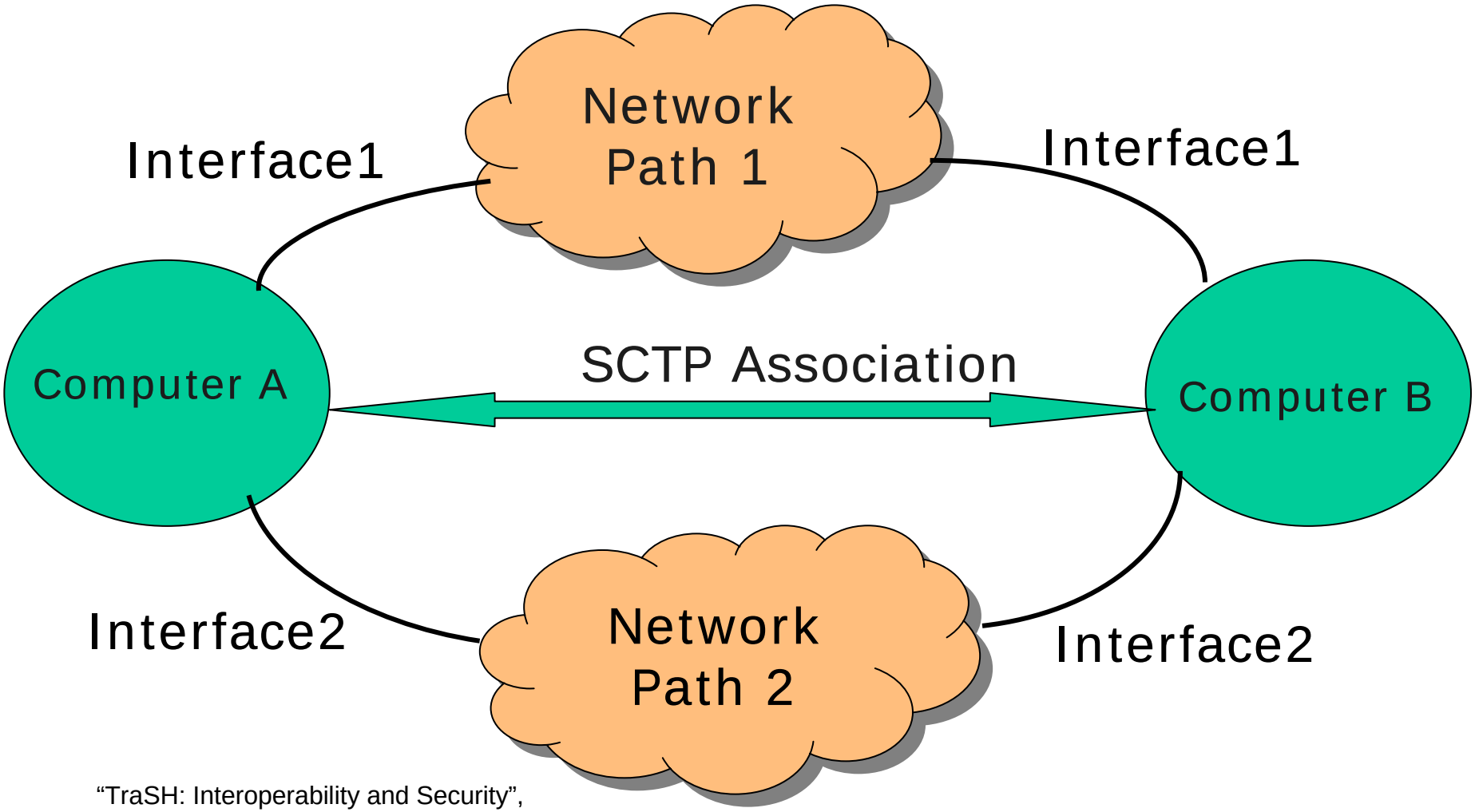
"TraSH: Interoperability and Security", Mohammed Atiquzzaman, IPCCC, April 2004

TCP and SCTP compared

- Both of them are reliable transport protocols;
- Similar Congestion Control algorithms (slow start, congestion avoidance);
- SCTP has two new features:
  - Multihoming
  - Multistreaming



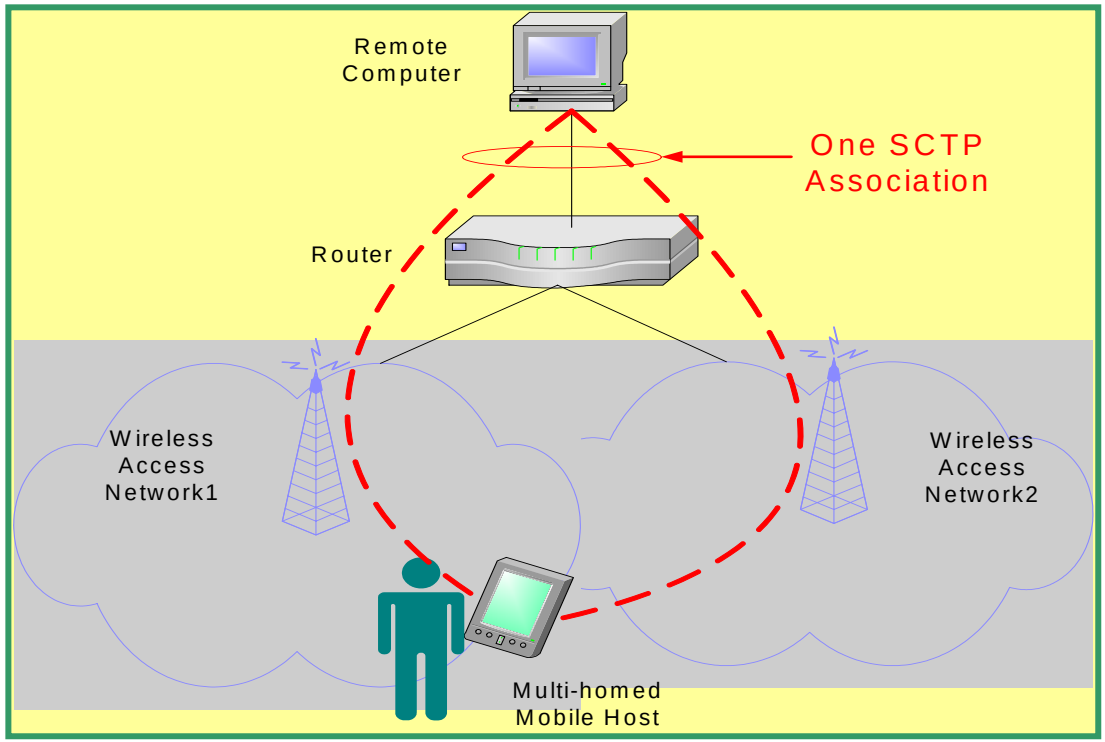
SCTP Multi-homing: Supporting Multiple IP Addresses in an Association.



"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

Basic concept of TraSH: Seamless Mobile Handover based on multihoming

- Mobile IP assumes the upper layer protocol use only one IP address to identify an logical connection. Some buffering or re-routing should be done at the router for seamless handover.
- SCTP support multiple IP addresses at transport layer naturally via multi-homing feature. When mobile host moving between cells, it can setup a new path to communicate with the remote computer while still maintaining the old path.



Advantages:

- Reduced packet loss and handover latency
- Increased throughput
- No special requirement on Routers

TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

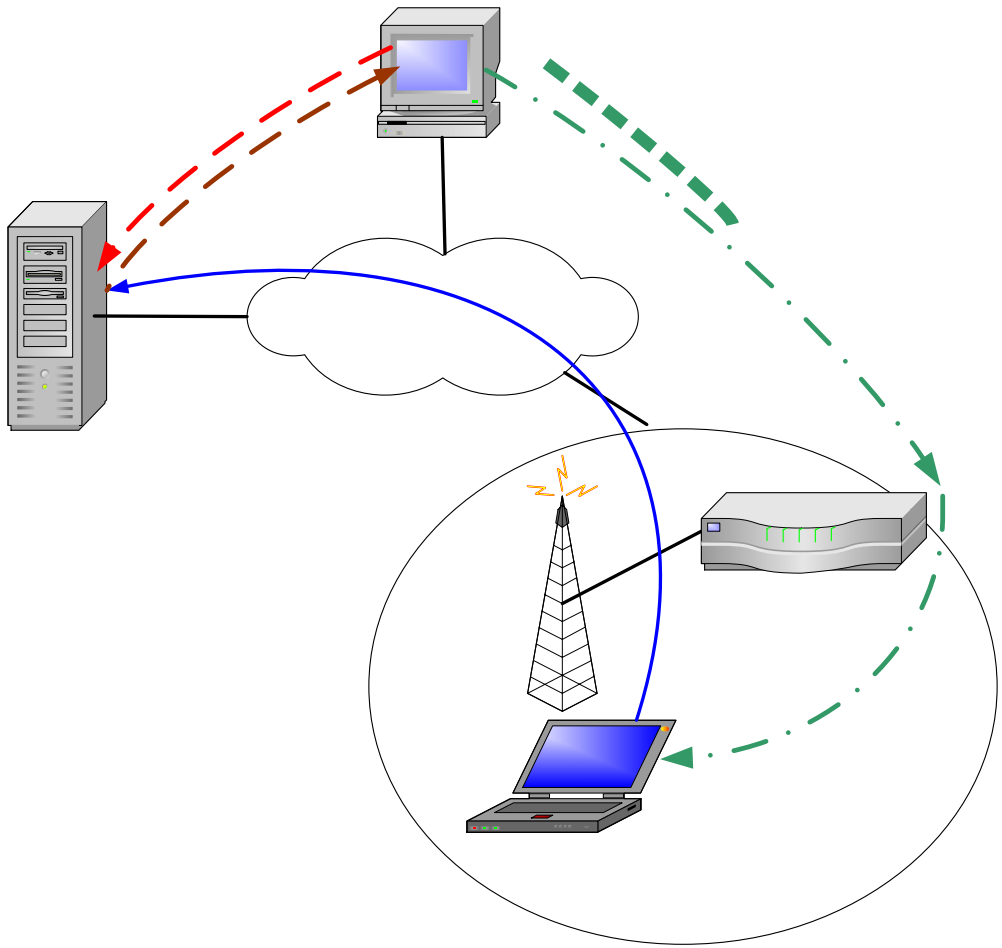
Security Threats in Mobile Networks

- Mobile communication faces all threats that are present in wired networks.
- Some specific issues introduced by the nature of wireless communication or user mobility:
  - Wireless communications is more vulnerable to eavesdropping
    - absence of a physical wire connection makes it easier to access services illegally.
    - Security association (SA) has to be re-established every time the mobile host moves into a new network, and secret key management/distribution becomes more difficult as peer identities can not be predetermined.

"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

Survivability of TraSH

- Only location update/query needs to be directed to Location Manager (LM). Thus LM need not to be located in a specific network.
- Easy to replicate LM at distributed secure locations to improve survivability.
- LM can further be integrated with DNS server to reduce system complexity.



"TraSH: Interoperability and Security", Mohammed Atiquzzaman, IPCCC, April 2004

More Benefits of Centralized Location Management

- Security: Storing user location information into a central secure databases is more secure than scattered among various Home Agents located at different sub-networks (in the case of Mobile IP).

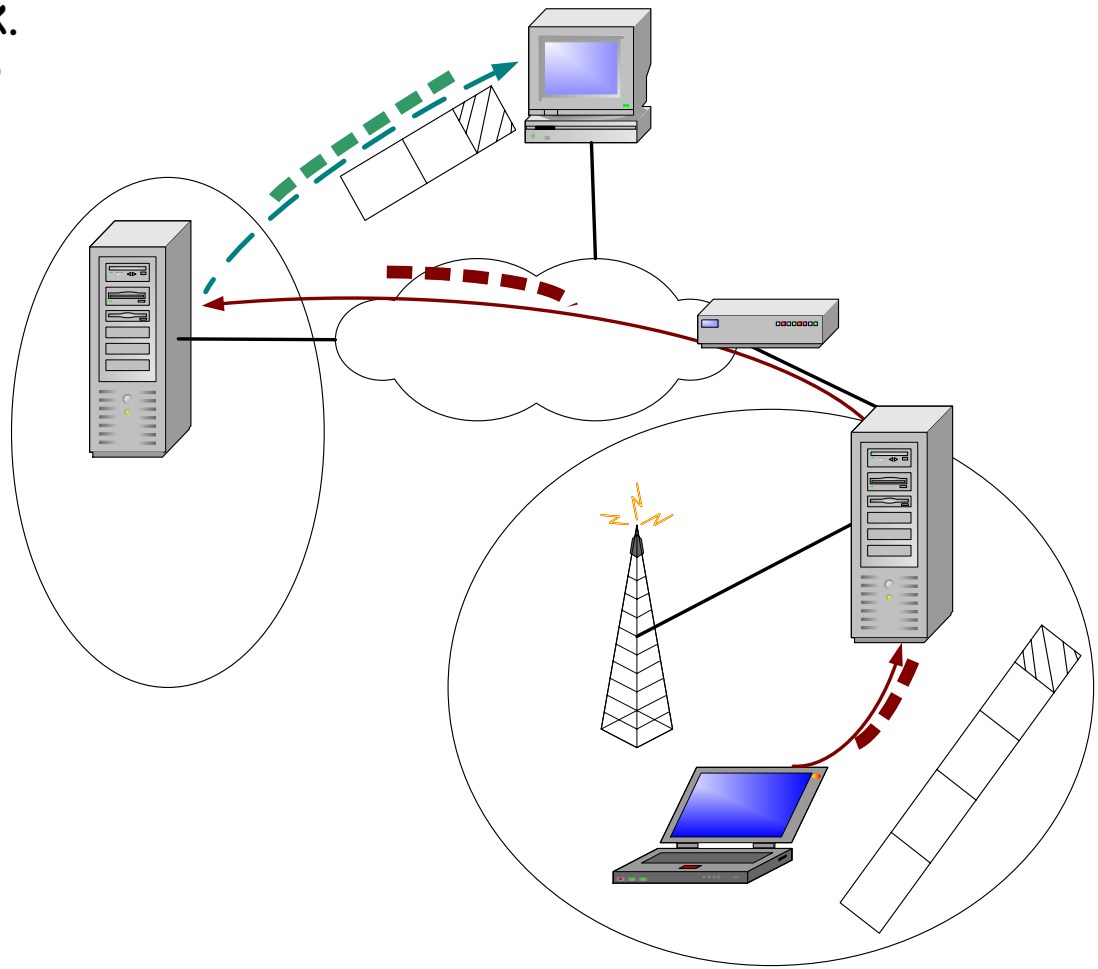
- Scalability: location servers do not intervene with data forwarding task, which adapts to the growth in the number of mobile users gracefully.

- Manageability: Centralized location management provides for an organization/service provider to control user accesses from a single server.

"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

Interoperate Mobile IP with Ingress Filtering

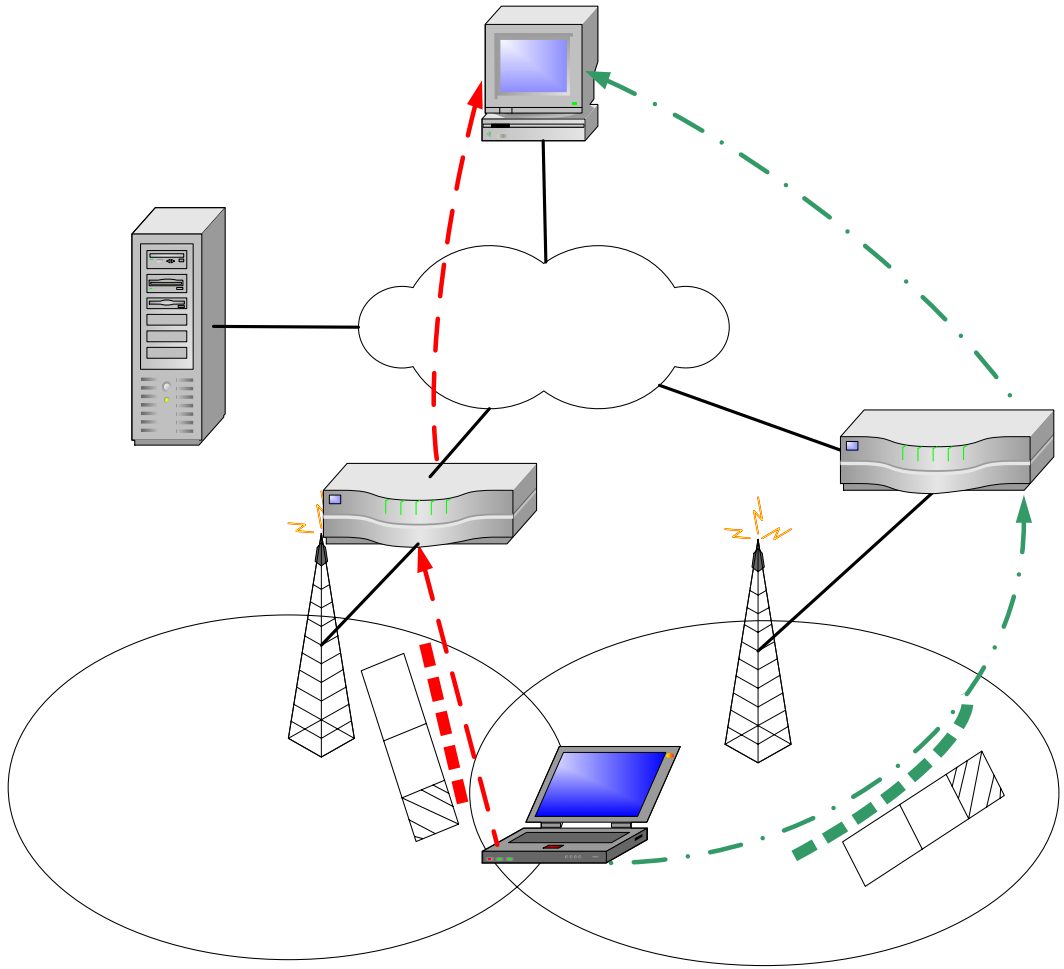
- Ingress filtering is heavily used in current Internet to prevent IP spoofing and DoS attack.
- Ingress filtering border routers enforce topologically correct source IP address.
- Topological correctness requires MH using COA as the source IP address.
- Applications built over TCP/UDP requires MH always using its home address as source address.
- **Solution: reverse tunneling**



"TraSH: Interoperability and Security", Mohammed Atiquzzaman, IPCCC, April 2004

Interoperate TraSH with Ingress Filtering

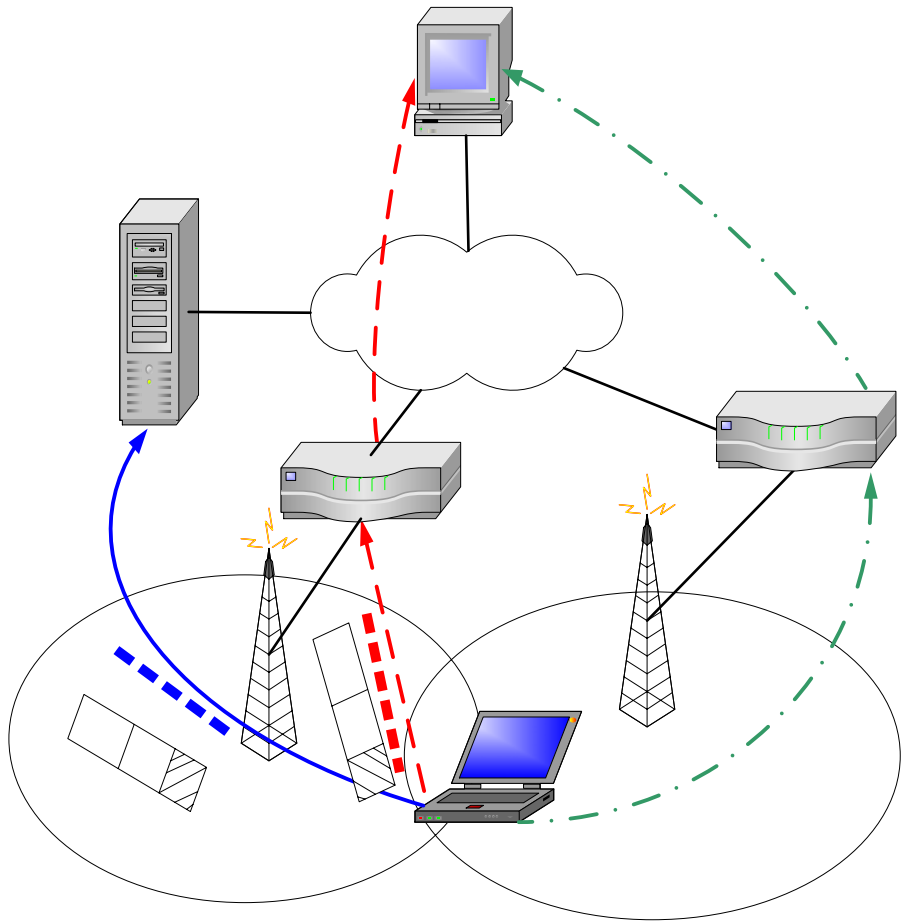
- In TraSH, MH uses new CoA address directly to communicate with CN, it is already topologically correct.
- TraSH can incorporate well with ingress filtering, no need for tunneling.



"TraSH: Interoperability and Security", Mohammed Atiquzzaman, IPCCC, April 2004

Increase the security of TraSH by IPSEC

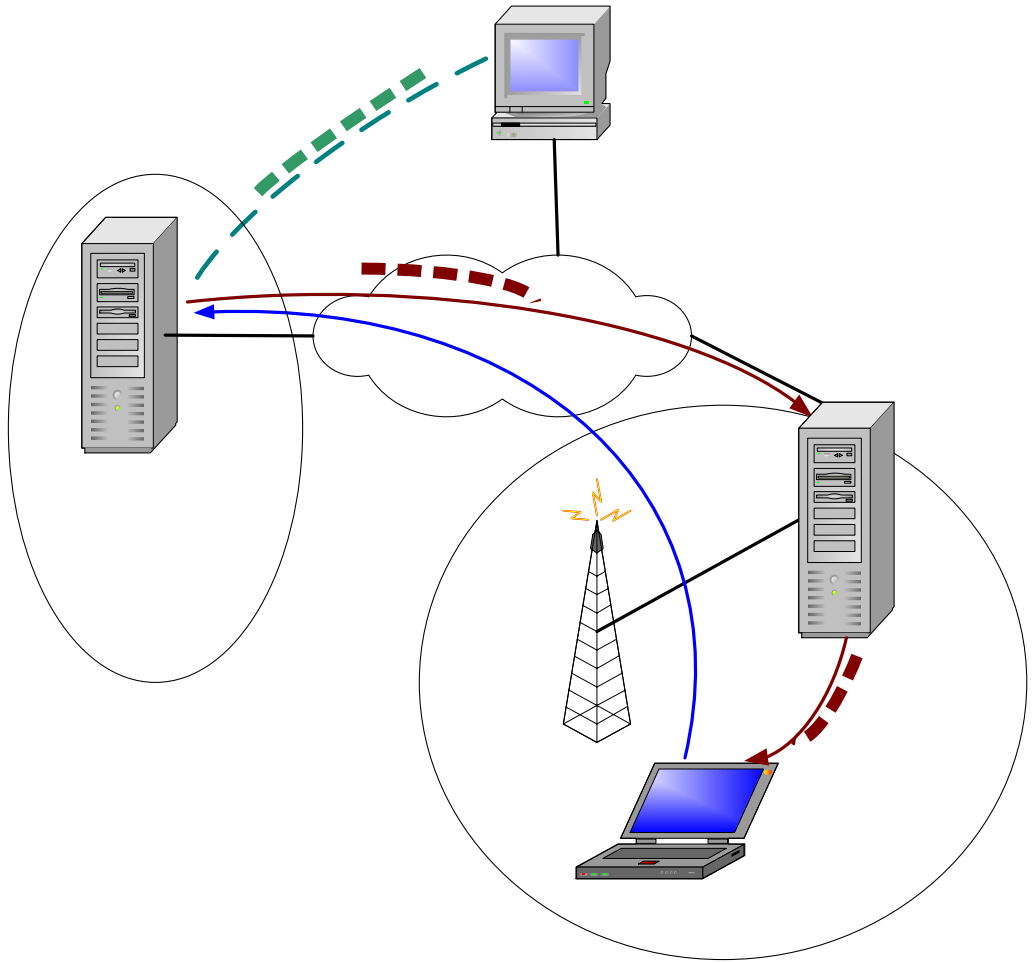
- TraSH depends on dynamic address reconfiguration
  - makes the association more vulnerable to be hi-jacked.
- Redirection attack: Bogus message sent by attacker to location manager
  - all further association setup messages will be sent to illegal IP addresses
- All location update and address reconfiguration messages sent to LM and CN should be protected by IPSEC AH header.



"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

Survivability issues introduced by location management of Mobile IP

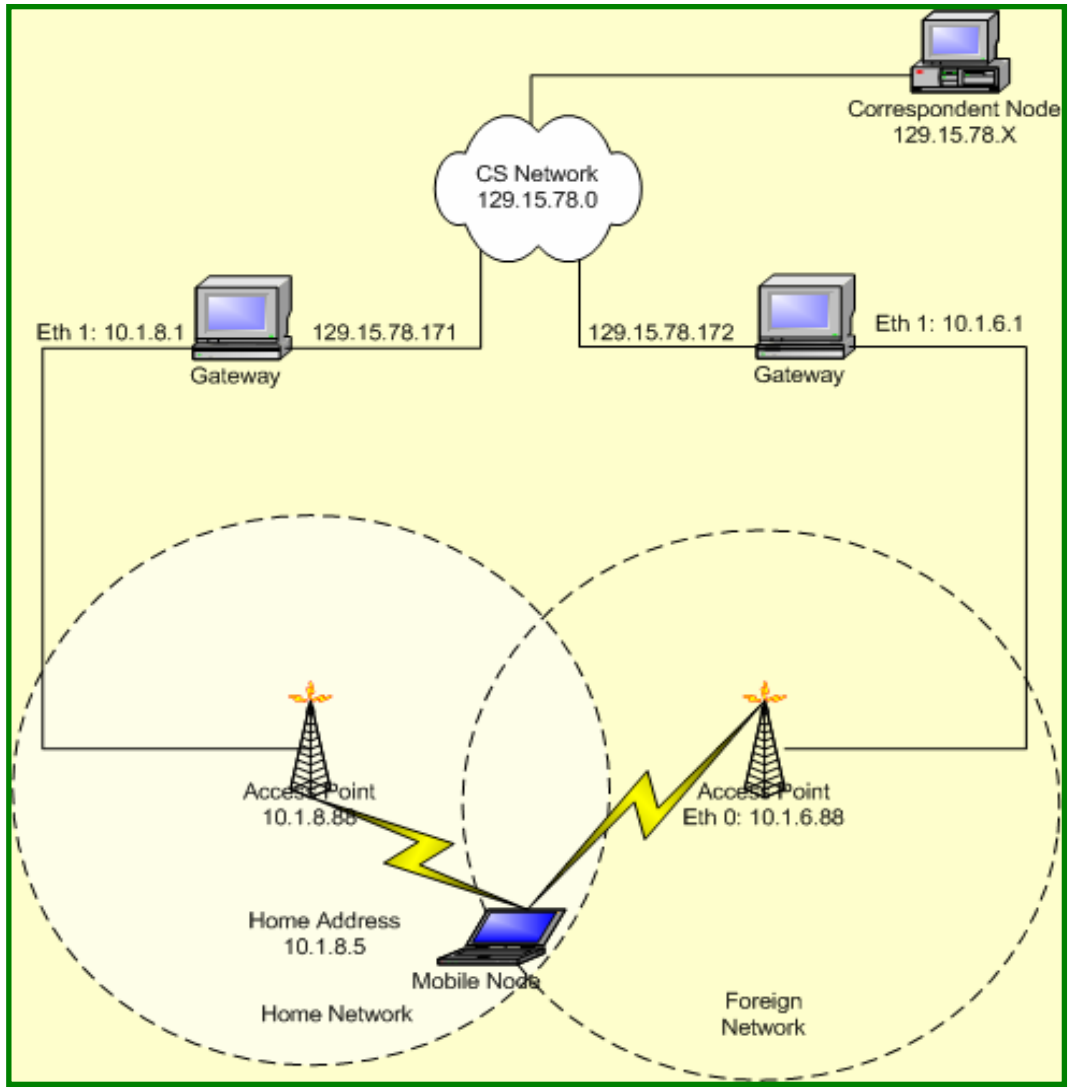
- In Mobile IP, Home Agent must reside in MH's home network to intercept packets sent from CN to MH.
- In situations where the home network is vulnerable to failure, this becomes a serious problem.
- It is difficult to replicate the Home Agent at various locations distributed throughout the network in order to achieve survivability.



"TraSH: Interoperability and Security", Mohammed Atiquzzaman, IPCCC, April 2004

TraSH Testbed

- lksctp reference implementation.
- Linux OS – Kernel 2.6.2.
- Network adapters
  - Avaya PCMCIA wireless network card and a NETGEAR USB wireless network card.

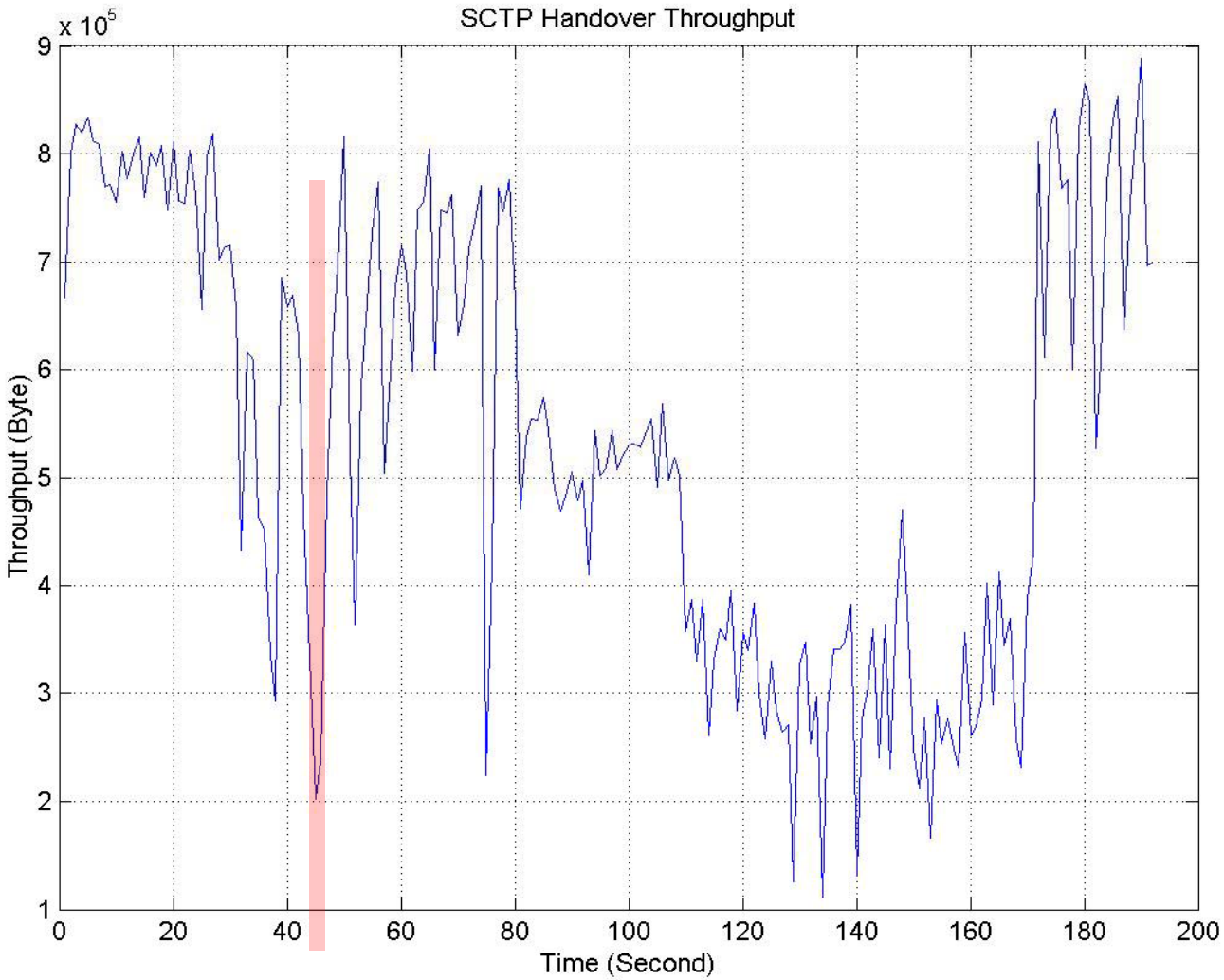


Operation of TRaSH:

- Link Layer is monitored to detect new AP signal strength.
- When a new AP is detected a new IP address is added to the association.
- When the new AP signal becomes stronger than the old AP signal, the Mobile Node notifies the Correspondent Node to make the new address the primary.

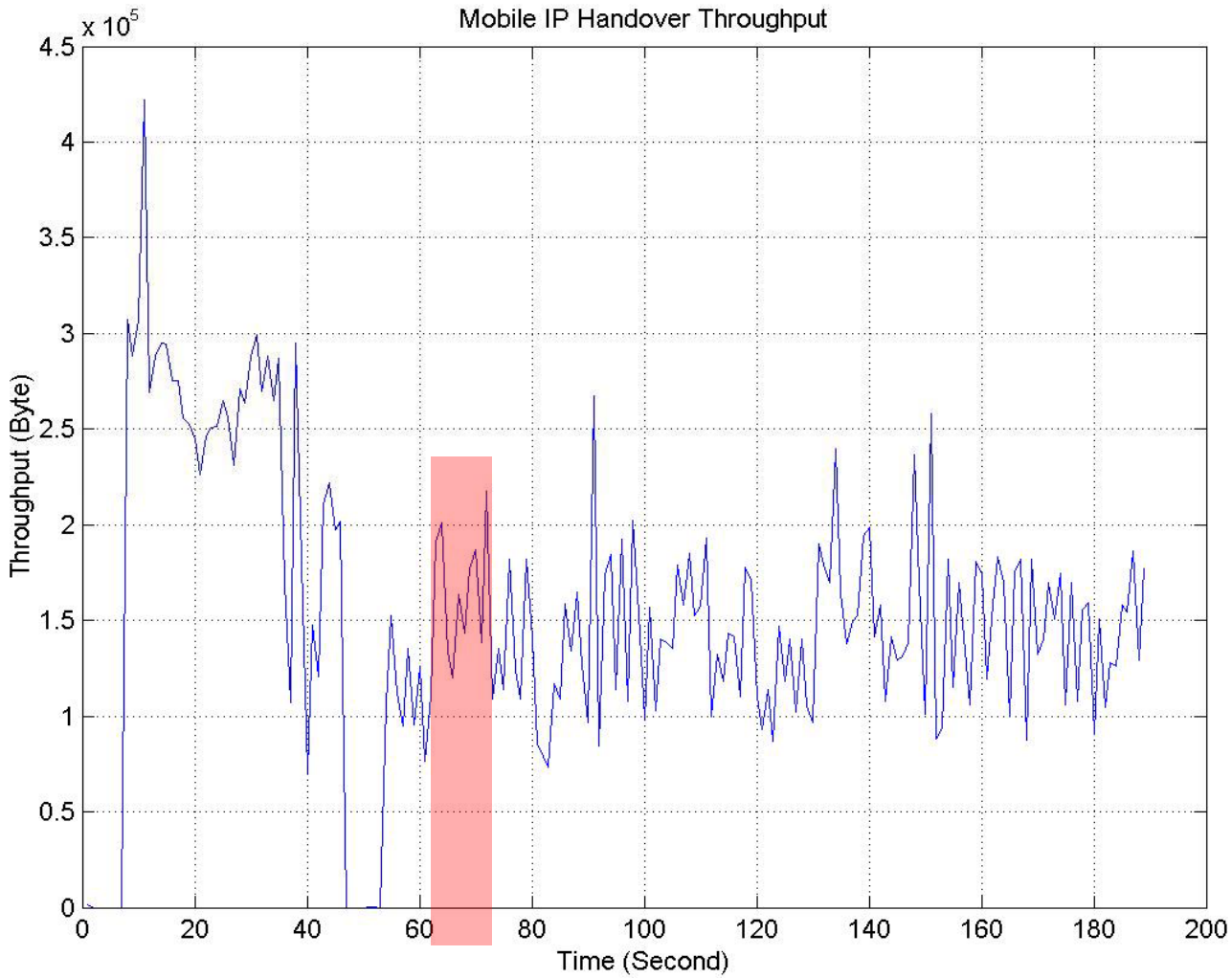
"TraSH: Interoperability and Security", Mohammed Atiquzzaman, IPCCC, April 2004

TraSH: Preliminary Results



"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

Mobile IP Results



"TraSH: Interoperability and Security",
Mohammed Atiquzzaman, IPCCC, April 2004

Some of the Open Research Issues of TraSH

- Interoperation of TraSH with firewalls and AAA servers.
- Efficient secret key management/distribution in TraSH.
- Apply TraSH into vertical handover.
- QoS related issues.

Acknowledgements

- National Aeronautics and Space Administration
- The following people are participating in the design, development and testing of TraSH:
  - Shaojian Fu
  - Liran Ma
  - Yong-Jin Lee
  - Justin Jones
  - Song Lu
  - William Ivancic

Further information: atiq@ou.edu

www.cs.ou.edu/~atiq