Workshop on Peer-to-Peer Multicasting

IEEE CCNC 2007

A Secure Multicast Model for Peer-to-Peer and Access Networks Using the Host Identity Protocol

Zueyong Zhu[†] and J. William Atwood[‡]

[†]University of Science and Technology of China

[‡]Concordia University, Montreal, Canada

Contents

- Introduction
- Motivation
- HIP Architecture
- Multicast Architectures
- Group Identification
- System Operation
- Validation
- Conclusion

Introduction

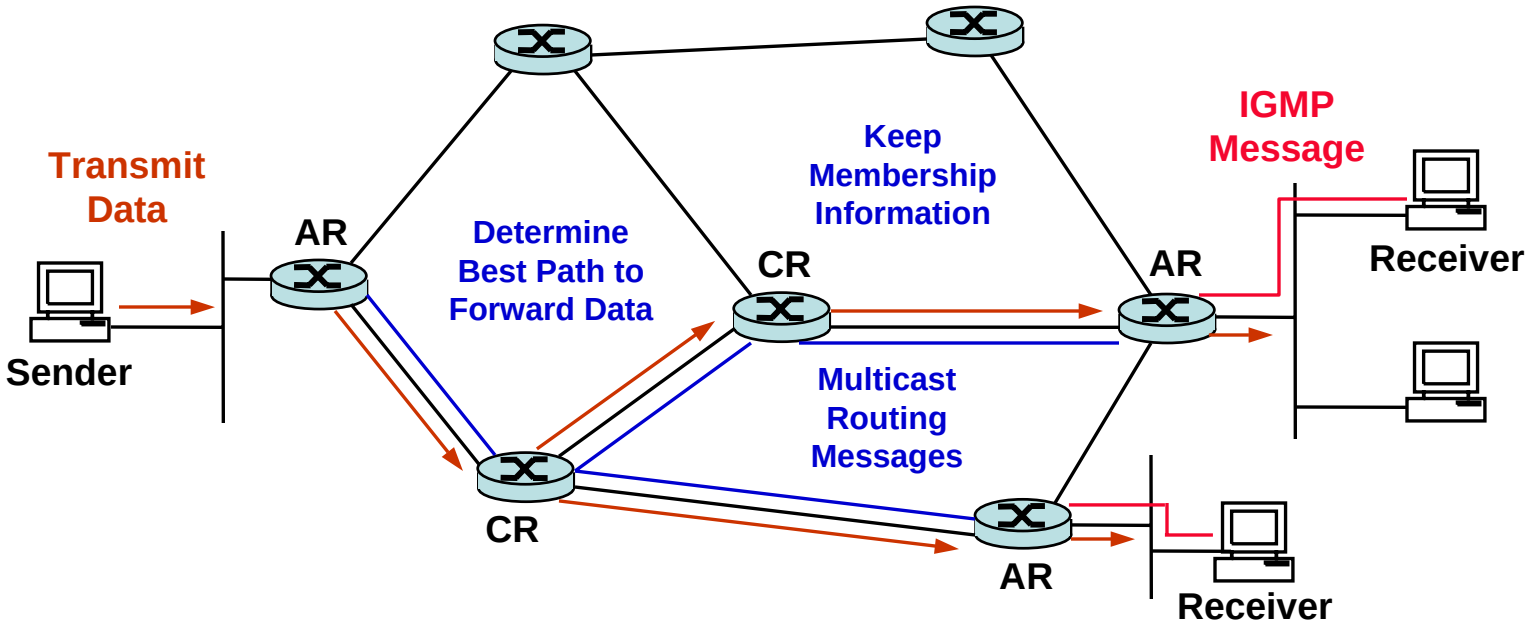


Figure 1: Present IP Multicast Architecture

Motivation

- Some applications need per-instance charging
- Not enough demand for multicast yet, to do this in native multicast
- Application Layer Multicast, Overlay Multicast
- Although general solutions may come, it is worthwhile to look at specific cases
- Two examples
  - xDSL
  - Collaboration

xDSL

- DSLAN <-> user is on a separate physical path
- Unicast gives same performance
- We gain:
  - Authentication
  - Secure access
  - Potential for accounting (revenue generation)

Wide Area Collaboration

- Strong need for authentication and authorization
- No need for accounting
- No revenue generation
- No benefit from multicast data transmission
- Overlay (p2p) multicasting is appropriate

No native multicast support

- When there is no native multicast support, we must use overlay or p2p

Host Identity Protocol

- Internet has two name spaces
  - (Fully Qualified) Domain Name
  - IP Address
    - Role as locator
    - Role as end-point identifier
- HIP separates these two roles
  - Host Identifier (public key, end-point id)
  - Host Identity Tag (128-bit hash, fixed-size end-point id)
  - 32-bit version exists for IPv4 environments
  - IP address continues to serve as locator

Host Identity Protocol ..2

- Host Identity Protocol
  - Authenticate participant hosts
  - Establish limited relationship of trust
- Four-packet Exchange
  - Initial packet (I1)
  - 3-packet Diffie-Hellman exchange (I2, R1, R2)

Multicast Architectures

- Overlay Multicast
  - Among participants
  - Independent of topology
  - All at application layer
- Native Multicast
  - Routers do it all
  - Source-based tree
  - Shared tree
- Agents
  - Packet duplication
  - Tree Management
  - Key Management
  - Authenticate group members
  - Collect accounting information

Our Cases

- P2P
  - HIP allows establishment of trust (security association) between the two unicast-linked nodes
  - Use any convenient tree-construction algorithm
- DSLAN
  - Unicast path
  - Host is initiator
  - Multicast Agent is on the DSLAN
  - Authentication via HIP

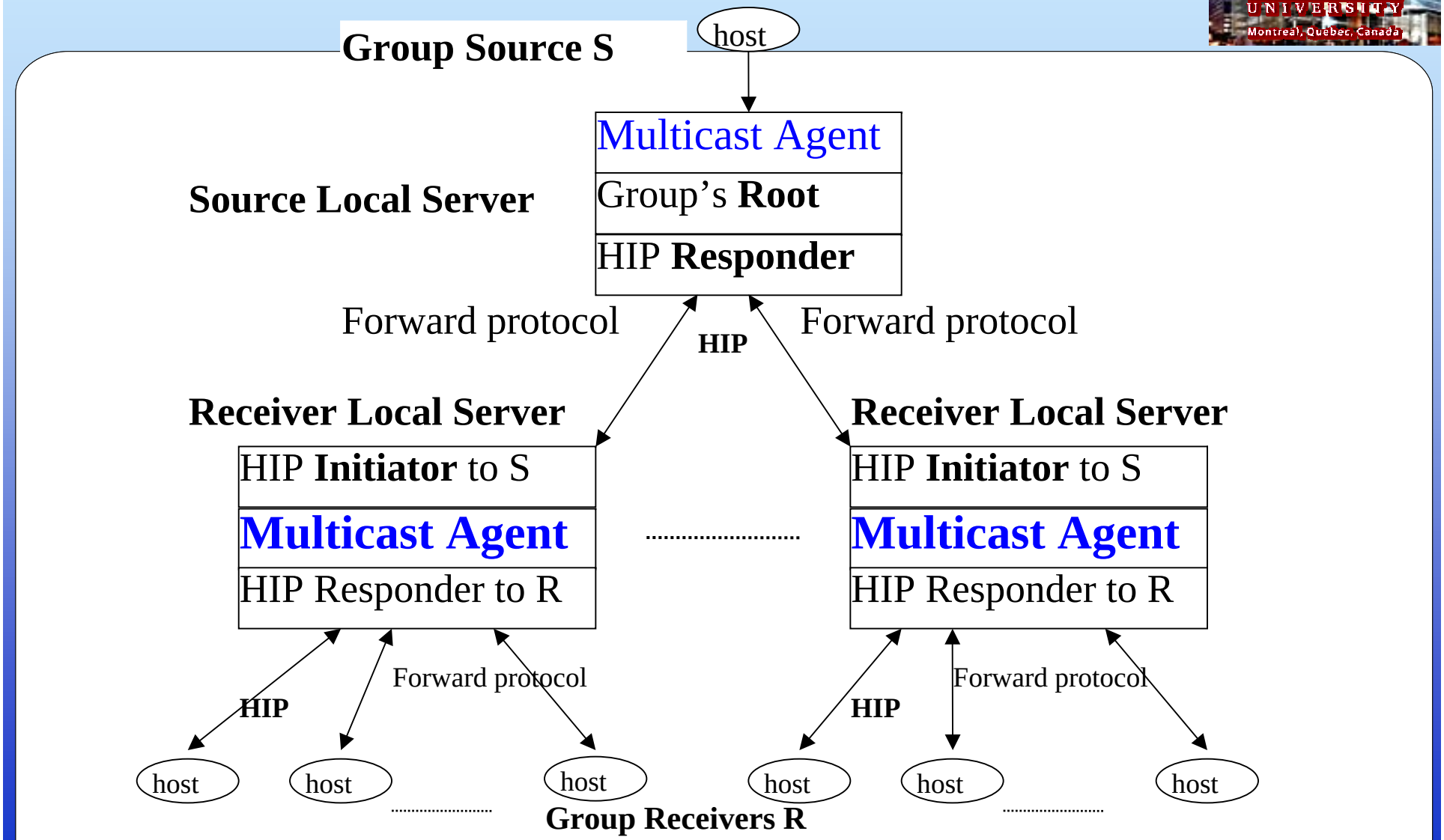
Advantages

- The security provided by HIP is just what we need
- Use of a Multicast Agent improves control in DSLAN

New Architecture

- Two-layer architecture (or n-layer)
- New interactions
  - No need for IGMP or PIM-SM
- Absolute control of membership

New Architecture



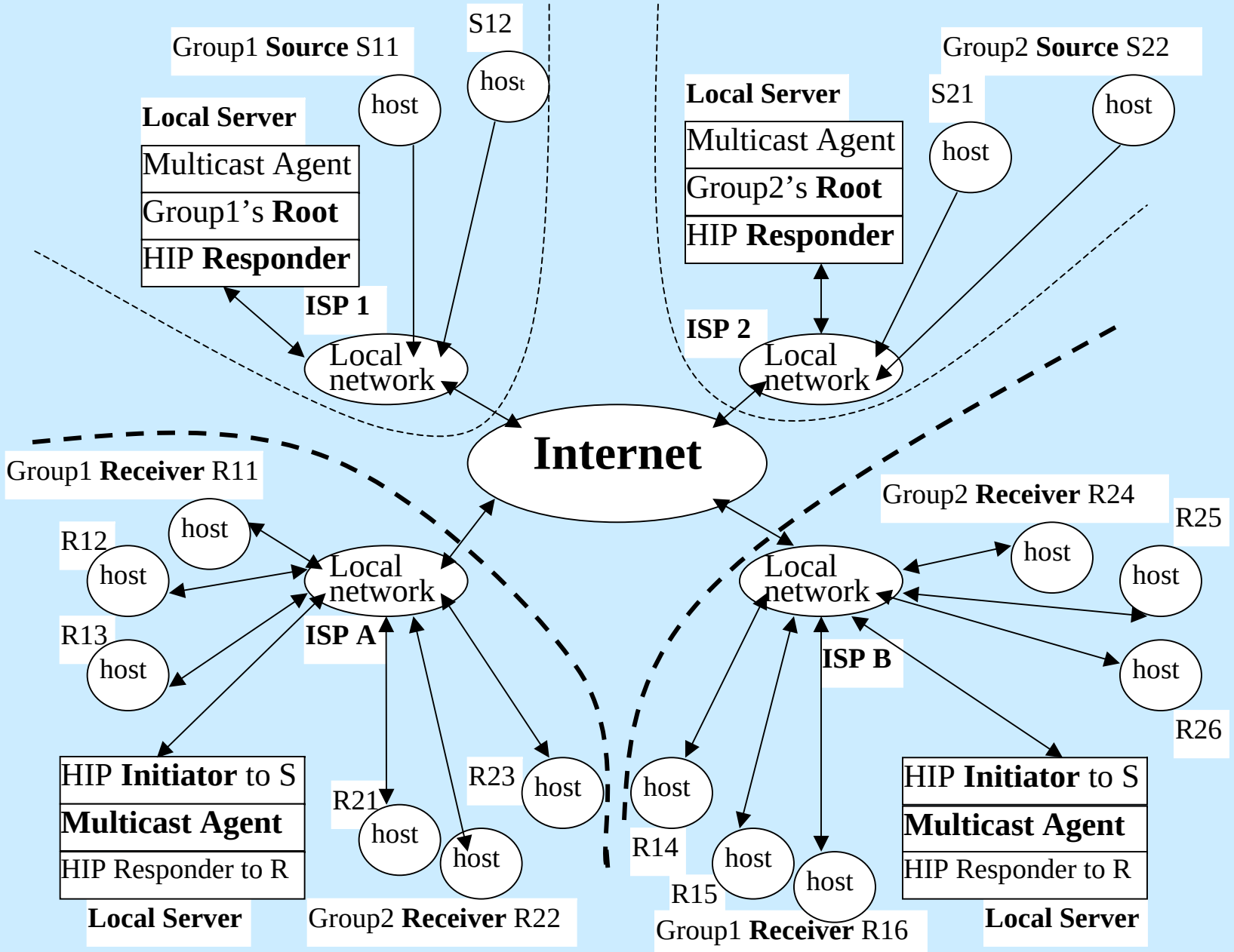
Identifying the Group

- Need a Group Identifier
- Structured identically to the Host Identifier and Host Identifier Tag: Group Identifier and Group Identifier Tag
- Extend I1 and R2 to carry the GIT
- I2 and R1 do not need to be changed

System Operation

- Join
  - Start HIP with your initiator (group receiver or MA)
  - Initiators join tree and receive multicast traffic
  - Responder joins tree or forwards to source
- Leave
  - Add “leaving request” parameter to HIP exchange
- Create
  - Add “create request” parameter to HIP exchange
- Two levels are independent

An example of application



Constructing Multicast Distribution Trees

- xDSL: One level of HIP-based control---MA joins the “native” multicast tree
- It is “trusted”, or native tree must be secure multicast
- Two-layer needs multiple unicast transmissions, or “snooping” in the network
- Can be extended to n-layer in the total absence of network support for multicast

Validation of the Model

- PROMELA + SPIN + Embeded C-code
- 32 receivers (Initiators)
- Some Intruders
- 2 Downstream MAs
- 1 Upstream MA
- 2 Senders
- Some routers

Results

- No assertion violation
- No invalid end-state
- No unreachable state
- No real, valid or successful attack
- Embeded C-code to test file transfer and simple encryption
  - Load not too great
  - Transfer is delayed, but not invalidated

Conclusion and future work

- Two new specialized architectures for multicast access control
  - One for peer-to-peer networks
  - One for xDSL environments
- Formal validation of its operation
- Future goals:
  - Incorporate into the global system that we are building

For more information

- High Speed Protocols Laboratory of Concordia University is doing extensive research on IP multicast,

  http://users.encs.concordia.ca/~bill/hspl/

- For questions and comments:

  zhuxy@ustc.edu.cn

  bill@cse.concordia.ca