Anonymous IP-Services via Overlay Routing

Simon Rieche , Olaf Landsiedel, Heiko Niedermayer,
Klaus Wehrle, Georg Carle

Protocol Engineering and Distributed Systems
University of Tübingen
http://ps.ri.uni-tuebingen.de

Outline

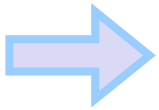
- **Motivation**
- **Related work**
- **Goals**
- **Anonymous communication**
  - Path concatenation scheme
  - Service Directory
  - Name Service
  - Transparent Application Support
- **Security analysis**
- **Example: anonymous web-browsing**
- **Conclusion**

Motivation

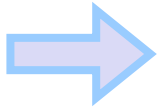
Every man should know that his conversations, his correspondence, and his personal life are private.

Lyndon B. Johnson
President of the United States
1963 – 69

Today: Communication in the Internet is not private



Access and provide information without the threat of personal consequences



Need for anonymous communication schemes providing sender and receiver anonymity

SARA: Sender And Receiver Anonymity

Related Work

	Web Mixes	Tor	Crowds	Tarzan	APFS	*SARA*
Relay	Server	Server	P2P	P2P	P2P	*P2P*
Anonymity	Sender	Sender, Receiver*	Sender	Sender	Sender, Receiver*	*Sender, Receiver*
Protocol	HTTP	TCP	HTTP	IP	Custom	*IP*

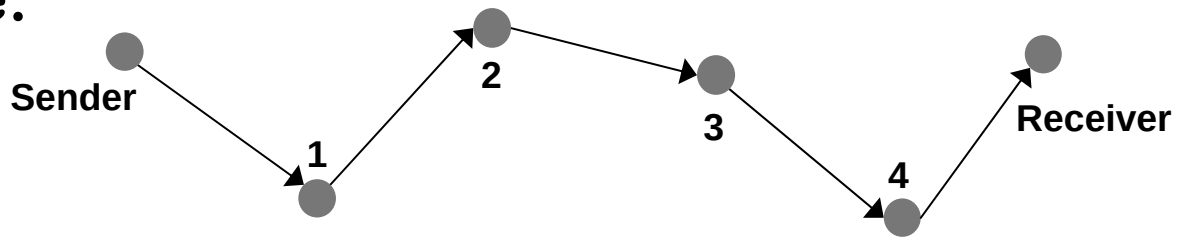
- **Pre setup channels via rendezvous points**
  - Do not depend on network load
  - Same for each everyone connecting to this server

Goals

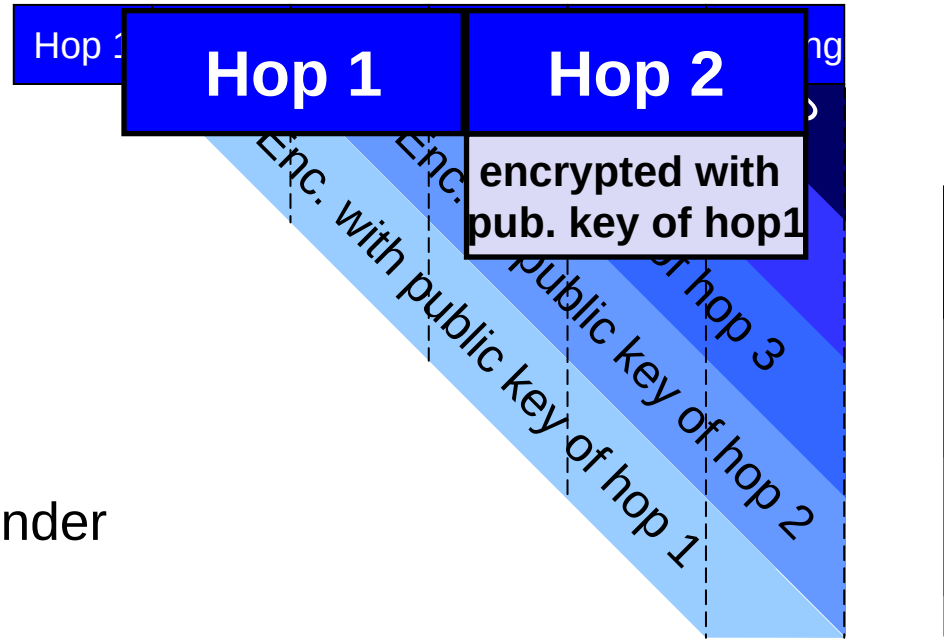
- **Sender and receiver anonymity**
- **Relationship anonymity**
- **Transparent application support**
  - No changes to applications
  - IP level sanitizing
- **Near real-time service**
- **Practical anonymity**
  - No protection against global eavesdropper

Anonymous Communication: Onion Routing

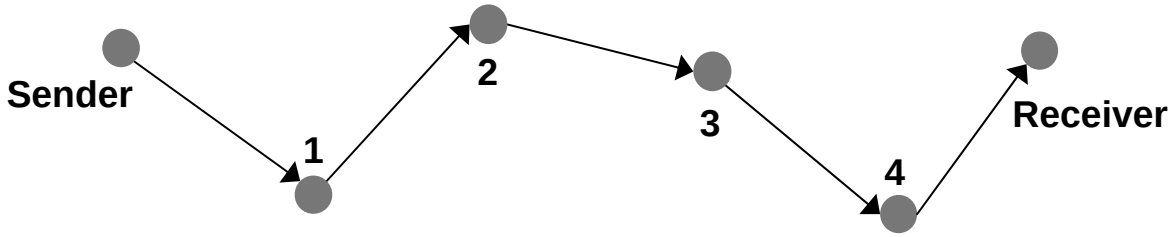
- **Example:**



- **Sender selects an anonymous path**
- **Layered encryption**
  - One hop can only decrypt its successor
  - Each hop removes a layer of encryption
  - Intermediate nodes and receiver have no information about the sender



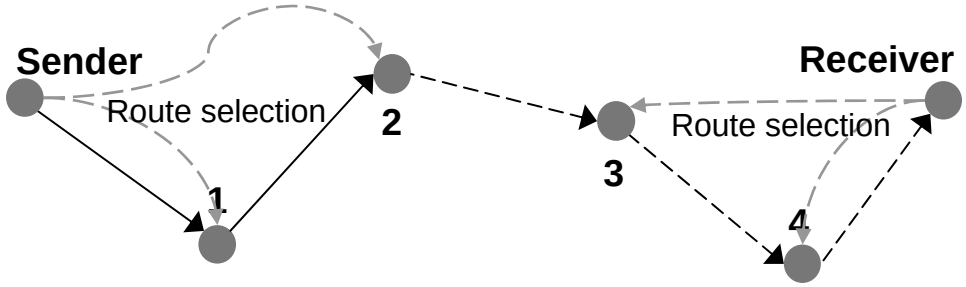
Anonymous Communication: Problem

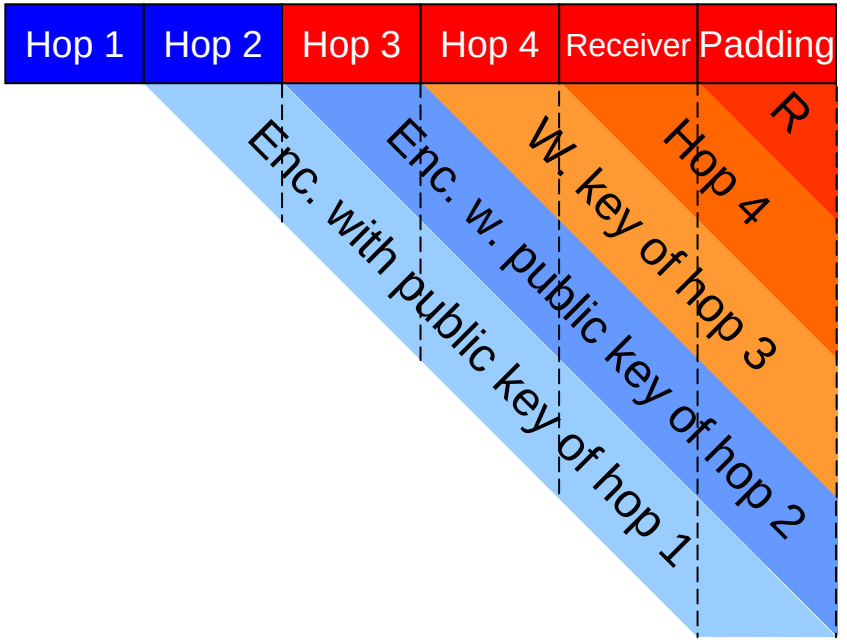


- **Sender has to know receiver's IP address**
  - Only sender and relationship anonymity
- **To provide receiver anonymity**
  - Hide receiver behind relaying nodes
  - Enables
    - Web server
    - File server
    - P2P

Anonymous Communication: Solution

- **Path selection**
  - Head by sender
  - Tail by receiver
- **Receiver publishes**
  - Path entry point
  - Path as layered encryption
- **Sender concatenates to anonymous path**





Service Discovery

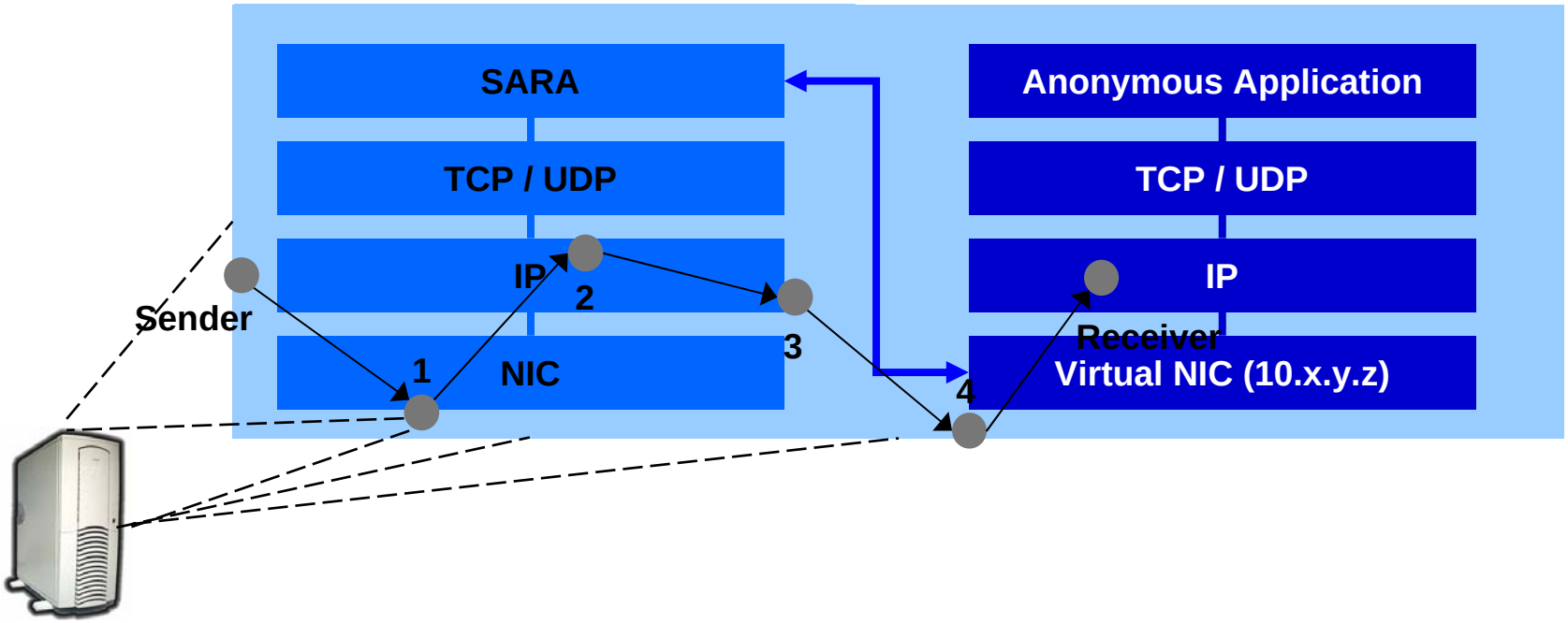
- **Retrieval of path sections**
- **The service discovery stores**
  - Anonymous path sections
    - Signed with anonymous id against impersonation
  - All relaying nodes
- **Path sections are encrypted**
  - Does not reveal
    - Relaying nodes' identities
    - Receiver's identity
  - Implementation choice
    - Trusted servers
    - Peer-To-Peer based index (e.g. Chord)

Transparent Application Support

- **Sanitizing**
  - Clear payload from personal information
- **In-band signaling**
  - Node IP in payload
  - FTP, H.323, real-audio….
- **Enhancement via proxy possible**
  - Very talkative protocols, like http
- **Other approaches only use proxies**

Transparent Application Support

- **Virtual network interface (NIC)**
- **Private IP address**
- **Application independent**
  - No changes to applications
  - Ftp, http, ssh, instant messaging, samba …



Threat Model

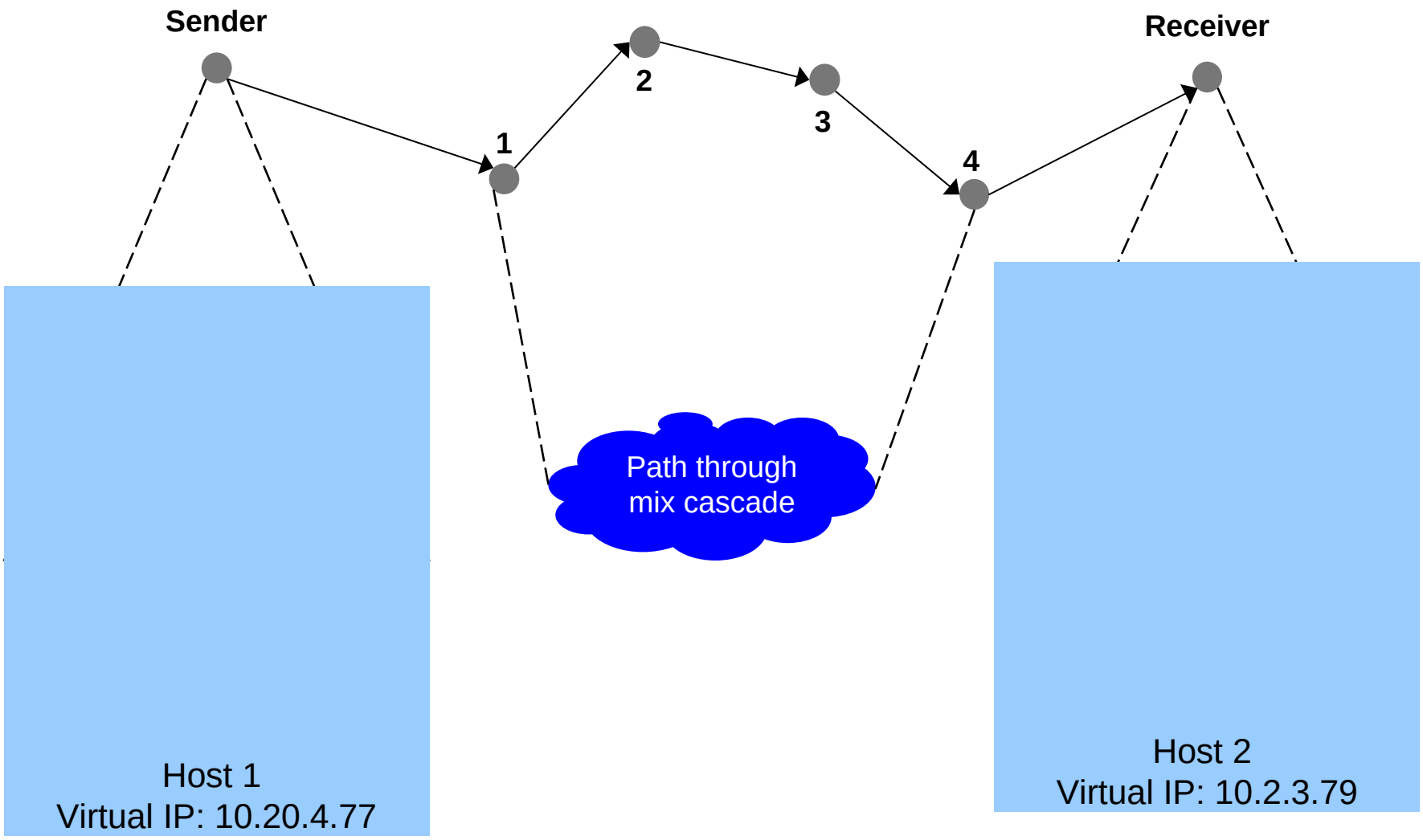
- **Practical adversary**
  - Observe some part of the network
  - Participate actively
    - Relaying traffic of other nodes
    - Offer service, e.g. web server
    - Access content
  - Compromise a limited number of nodes
  - Influence communications
    - Generating,
    - Delaying,
    - Modifying traffic content and patterns
- **Do not protect against global adversary!**

Security Analysis

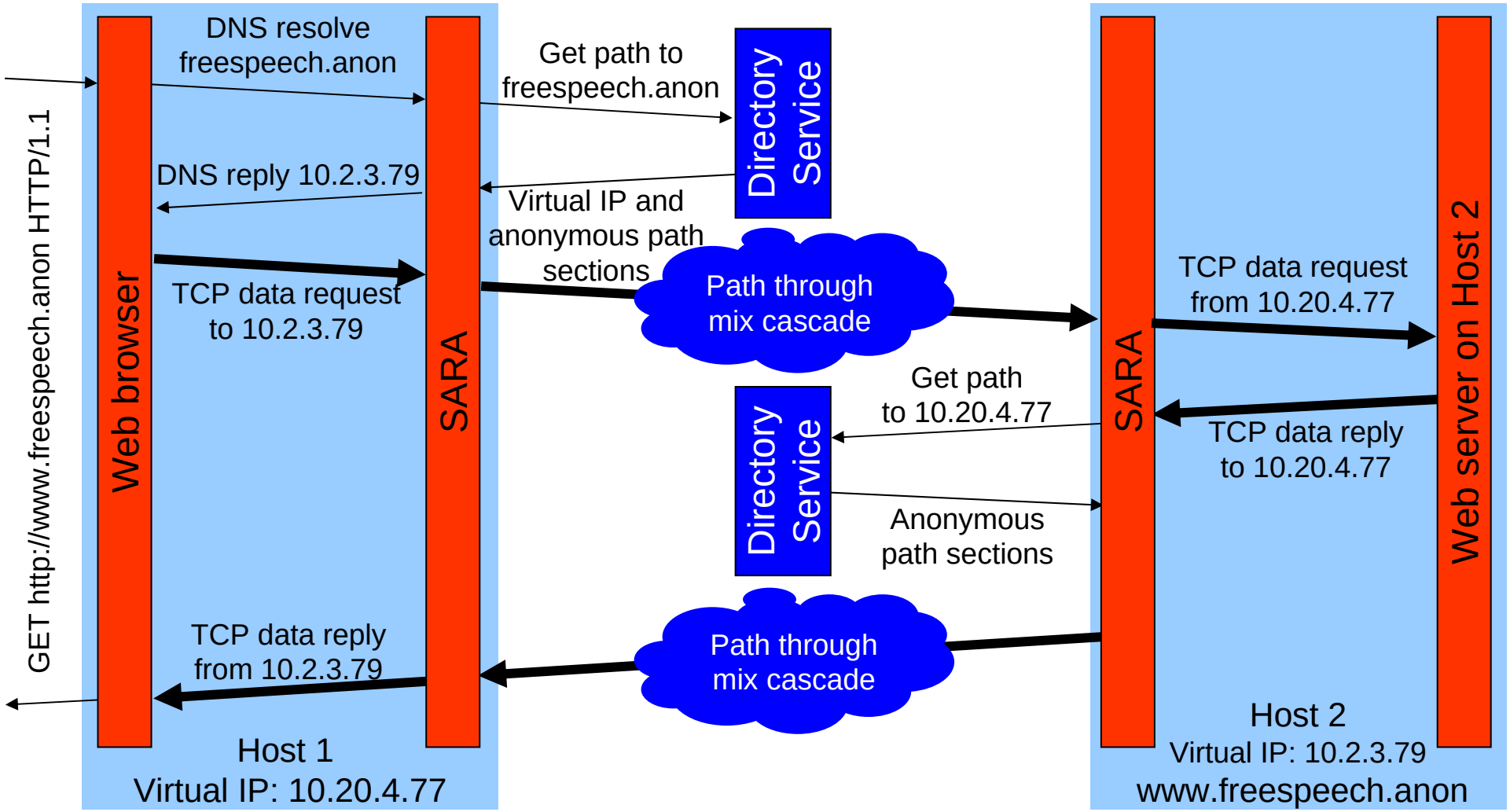
- **Source / destination observation**
  - Traffic is relayed
  - Traffic relay for other nodes
  - Messages padding to constant length,

⇨ It is not possible to determine via observation whether a node is sender, relay or receiver of a message.

Example: Using a Web Browser



Example: Using a Web Browser

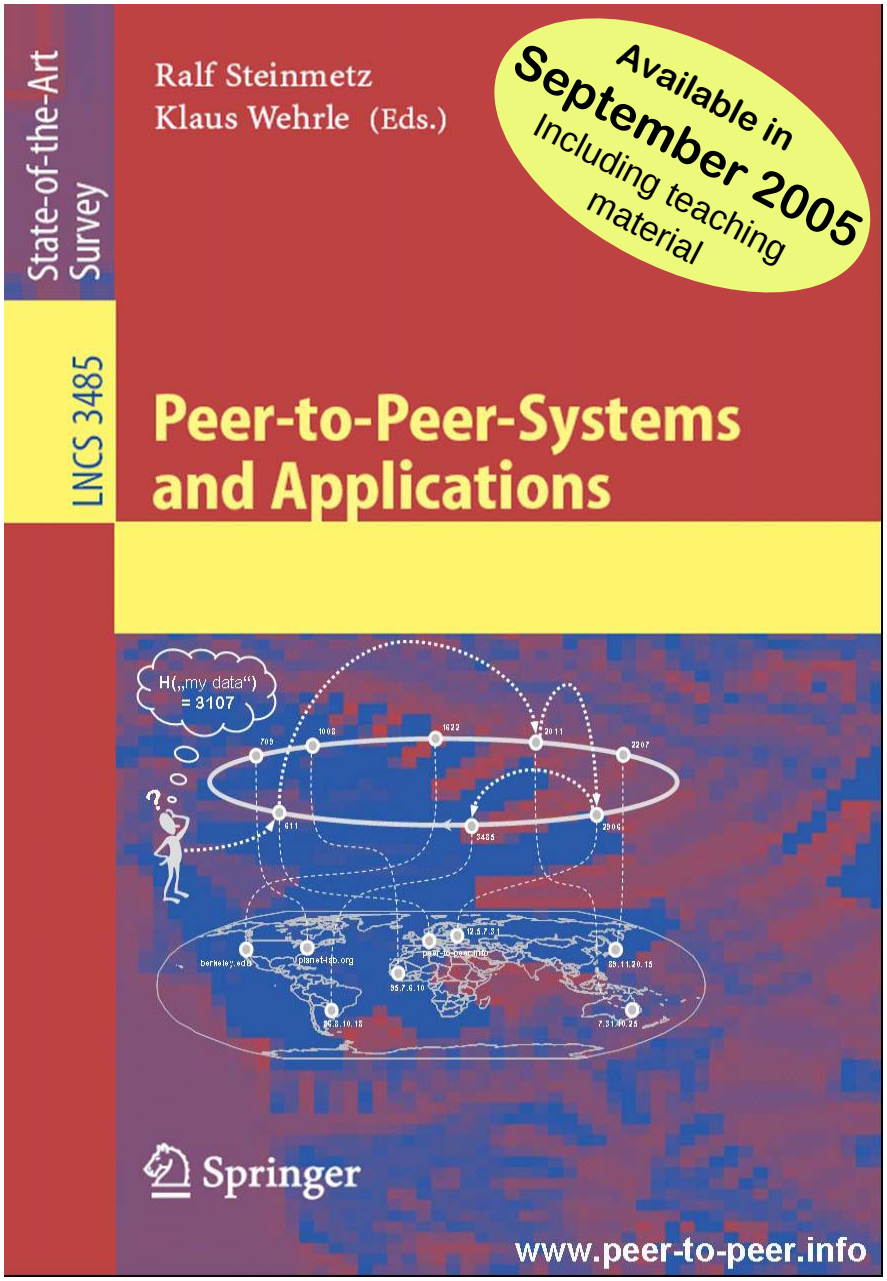


Conclusion

- **Need for**
  - Sender and receiver anonymity
  - Transparent application support
- **SARA provides**
  - Sender, receiver, and relationship anonymity
  - Via path concatenation
- **Transparent application support**
  - Communication stack, IP level support
  - Address virtualization
  - Seamless support for most protocols / applications
- **Integration of existing web applications**
  - Web and fileservers
  - Instant messaging, Audio streaming

Time for questions

http://ps.ri.uni-tuebingen.de



Ralf Steinmetz, Klaus Wehrle (Eds.)

Peer-to-Peer Systems & Applications

Springer Publishing, Sept. 2005

- **Compendium**
  - 10 Parts / 32 Chapters / 650 pages
  - Covers the wide spectrum of Peer-to-Peer Systems and Applications
- **Text Book for Teaching:**
  - Chapters designed for teaching classes and seminars
  - eLearning material available
- **Web Site:**
  - http://www.peer-to-peer.info