Naming Architecture for the Next Generation Internet

Jianli Pan, Subharthi Paul, Raj Jain

Professor of Computer Science and Engineering

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

These slides and Audio recordings of the talk are at:

http://www.cse.wustl.edu/~jain/talks/naming.htm

Acknowledgement

This research is made possible by a grant from Intel Research Council

- Internet 3.0
- Problems with the Current Internet
- MILSA Architecture
- User- Host- and Data Centric Models
- Policy Oriented Naming Architecture

Internet 3.0

- National Science Foundation is planning a $300M+ research and infrastructure program on next generation Internet
  - Testbed: "Global Environment for Networking Innovations" (GENI)
  - Architecture: "Future Internet Design" (FIND).
- Q: How would you design Internet today? Clean slate design.
- Ref: http://www.nsf.gov/cise/cns/geni/
- Most of the networking researchers will be working on GENI/FIND for the coming years
- Internet 3.0 is the name of the Washington University project on the next generation Internet
- Named by me along the lines of "Web 2.0"
- Internet 3.0 is more intuitive then GENI/FIND

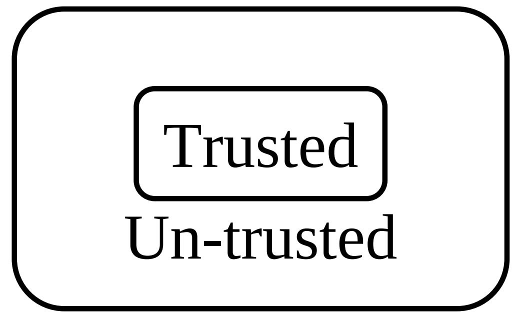
Problems with the Current Internet

1. Security:

a. Designed for research ⇒ Trusted systems
Used for Commerce ⇒ Untrusted systems

b. Control, management, and data path are intermixed ⇒ security issues.

c. Perimeter based security
Trust everything inside the perimeter
Do trust anything outside the perimeter
Can’t reach inside from outside



d. Difficult to represent organizational, administrative hierarchies and relationships

Problems (cont)

2. Mobility

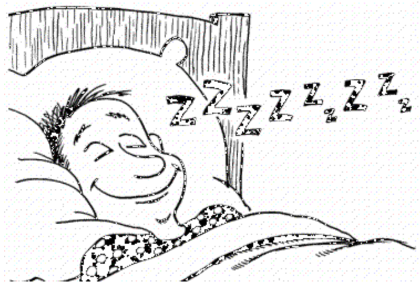
a. Identity and location in one (IP Address)
Makes mobility complex.

b. IP address changes with location
but can not determine location
⇒ Most services require nearest server
⇒ Also, Mobility requires location

c. Single-interface to single-interface communication
⇒ Difficult to represent globally distributed systems and services

d. No representation for real end system: the human.

Problems (cont)



3. Energy Efficiency:

a. Assumes live and awake end-systems and intermediate systems

b. Does not allow communication while sleeping.Many energy conscious systems today sleep.

Names, IDs, Addresses

Name: John Smith

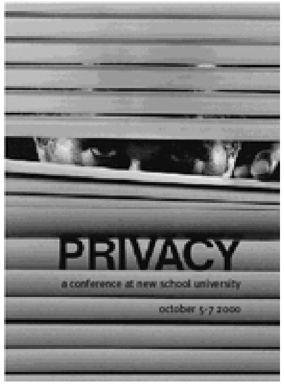
ID: 012-34-5678

Address:
1234 Main Street
Big City, MO 12345
USA

- Address changes as you move, ID and Names remain the same.
- **Examples**:
  - Names: Company names, DNS names (Intel.com)
  - IDs: Cell phone numbers, 800-numbers, Ethernet addresses, Skype ID, VOIP Phone number
  - Addresses: Wired phone numbers, IP addresses

More Problems with IP Addressing

- Multihoming is not properly represented
  - TCP is bound to an IP address. If one port fails, TCP gets disconnected.
- Private IP addresses behind NAT boxes are not reachable from outside
- Mobile IP can provide either location privacy by triangulation or route optimization with no location privacy



A Sampling of Id-Address Solutions

- **Host Identity Protocol (HIP):**
  - Uses a hash of the host public key as the host ID
  - Solves the host authentication problem
  - No concept of logical and organizational relationships
- **Internet Indirection Infrastructure (I3):**
  - Hash of the ID tells you where to go to find the address
  - Addresses mobility but without security
  - The rendezvous server may not be trusted by client
- **Shim6**:
  - Solves the problem of multi-homing
  - Uses one of the IPv6 addresses as identifier
  - Does not handle mobility or security.
- **LISP**, **GSE**, ….See our Survey of Naming Systems

Internet 3.0 Naming Architecture: MILSA

- Multihoming supporting Identifier Locator Split Architecture
- Designed for security, mobility, and fault tolerance
- Separates trust (logical) relationships from physical connectivity
- Separates control from data plane
- Layer 3.5 $\Rightarrow$ Features available to all applications
- Supports multi-homing
- Works with current IP Routing $\Rightarrow$ Easy to transition

Physical vs. Logical Connectivity

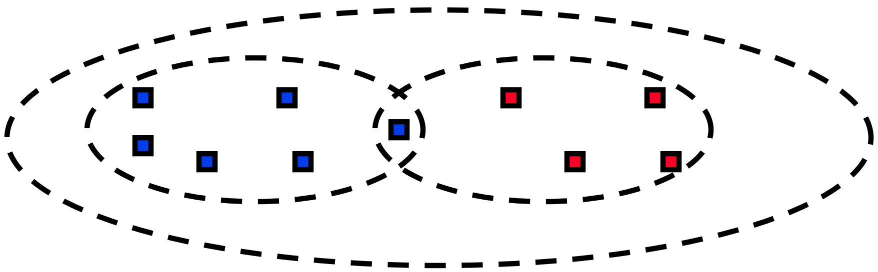
- Physically and logically connected: All computers in my lab = Private Network, Firewalled Network

- Physically disconnected but logically connected: My home and office computers

- Physically connected but logically disconnected: Passengers on a plane, Neighbors, Conference attendees sharing a wireless network, A visitor

Physical connectivity ≠ Trust

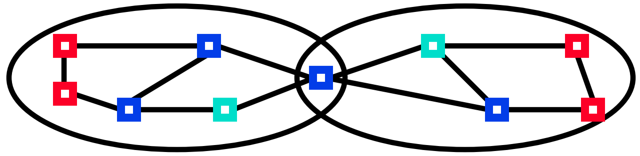
Realms



- Object names and Ids are defined within a realm
- A realm is a **logical** grouping of objects that have a certain level of **trust**
- A realm represents an organization
  - Objects inside the realms communicate with each other at a higher level of trust than with objects outside the realms
  - Objects can be and generally are members of multiple realms
  - Realm managers set policies for communications
  - Realm members can share services.
- Realm Boundaries: Organizational, Technological, Governmental, ISP

Realm = Organization

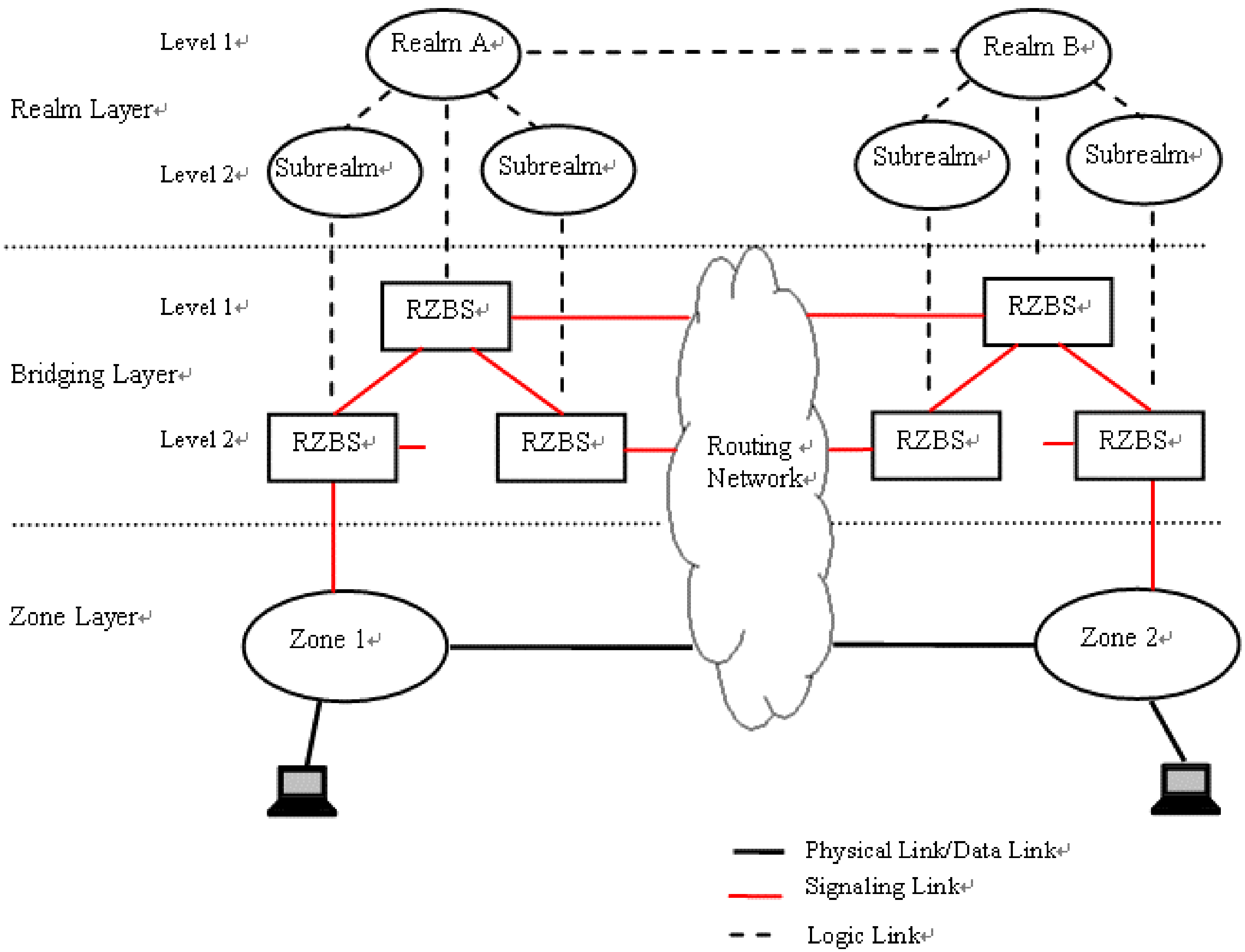
Zones



- Address of an object indicates its ***physical attachment point***
- Networks are organized as a set of ***zones***
- Object address in the current zone is sufficient to reach it inside that zone
- Zones are **physical** grouping of objects based on connectivity. Does not imply trust.

Zonal Hierarchy = Network Structure

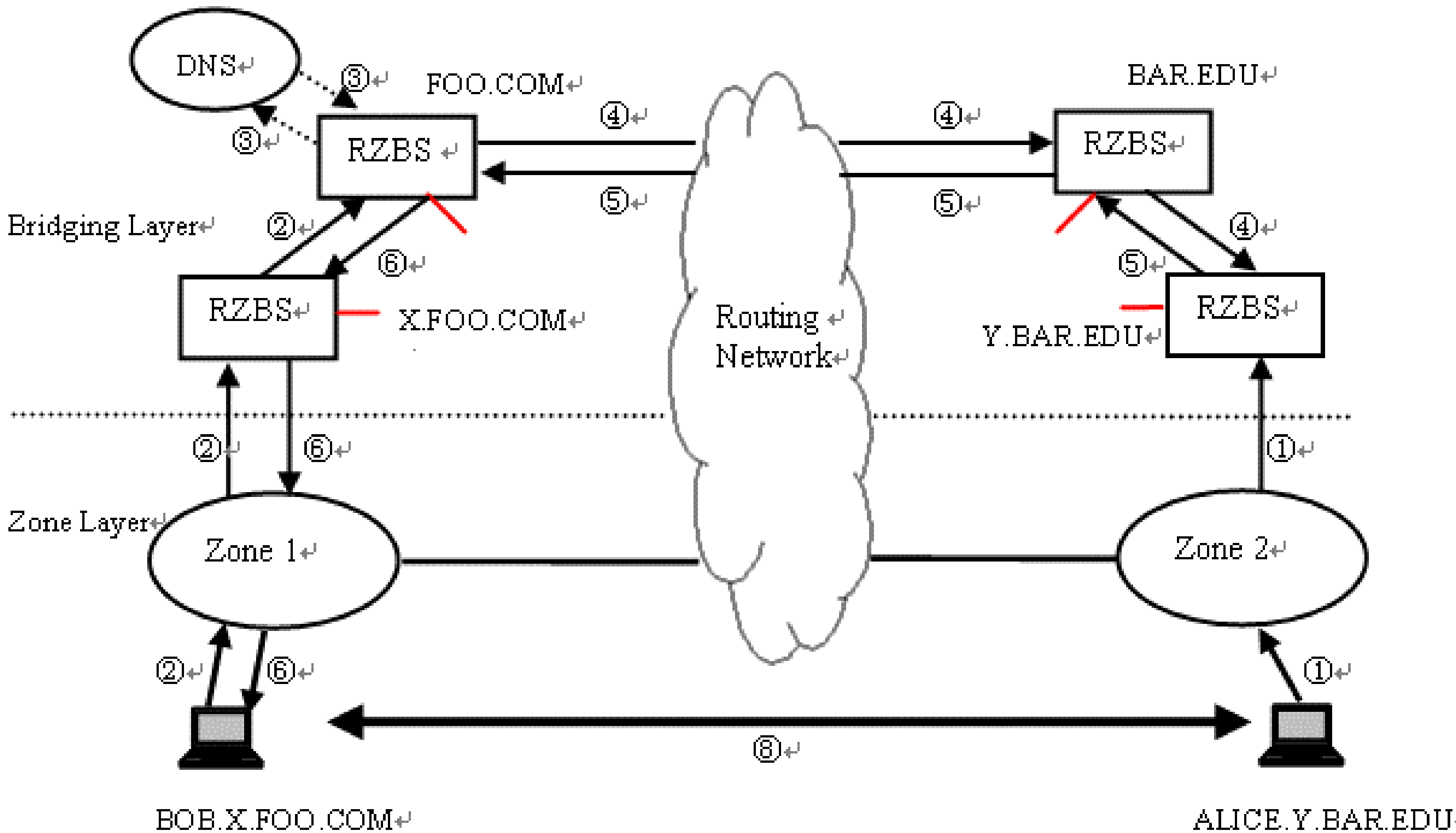
MILSA Architecture



MILSA Architecture: Key Features 1

- Hierarchical URI-like Identifiers (HUI):
  e.g., bob.x.foo.com
- Realm-Zone Bridging Server (RZBS):
  Provides the name to address translation
- Trust Relationship: RZBS belong to a realm and have trust relationships with its clients and higher level RZBSs. Set up trust relationship with other RZBSs as needed.

System Scenario - Connection Setup



Connection Setup (Cont)

1. Bob.x.foo.com registers with RZBS x.foo.com
   Alice.y.bar.edu registers with its RZBS y.bar.edu
2. Bob wants to talk to Alice ⇒ Bob sends a resolution request to its RZBS x.foo.com, which forwards it to RZBS foo.com
3. RZBS foo.com sends a DNS query for the address of RZBS bar.edu
4. RZBS foo.com sets up a trust relationship with RZBS bar.edu and forwards the resolution request to it. RZBS bar.edu forwards it to RZBS y.bar.edu
5. RZBS y.bar.edu returns the current address of Alice to RZBS Foo.com
6. RZBS Foo.com forwards it to Bob.
7. Bob sets up a direct connection with Alice

MILSA: Key Features 2

- Control and data plane separation:
  RZBS is used only in the control plane
- DNS is used only for RZBS's address which are static
- A node can register multiple interfaces (addresses) in multiple zones with a RZBS $\Rightarrow$ Multihoming
- Object Proxy:
  A node can register any other node as proxy
  $\Rightarrow$ Allows location privacy

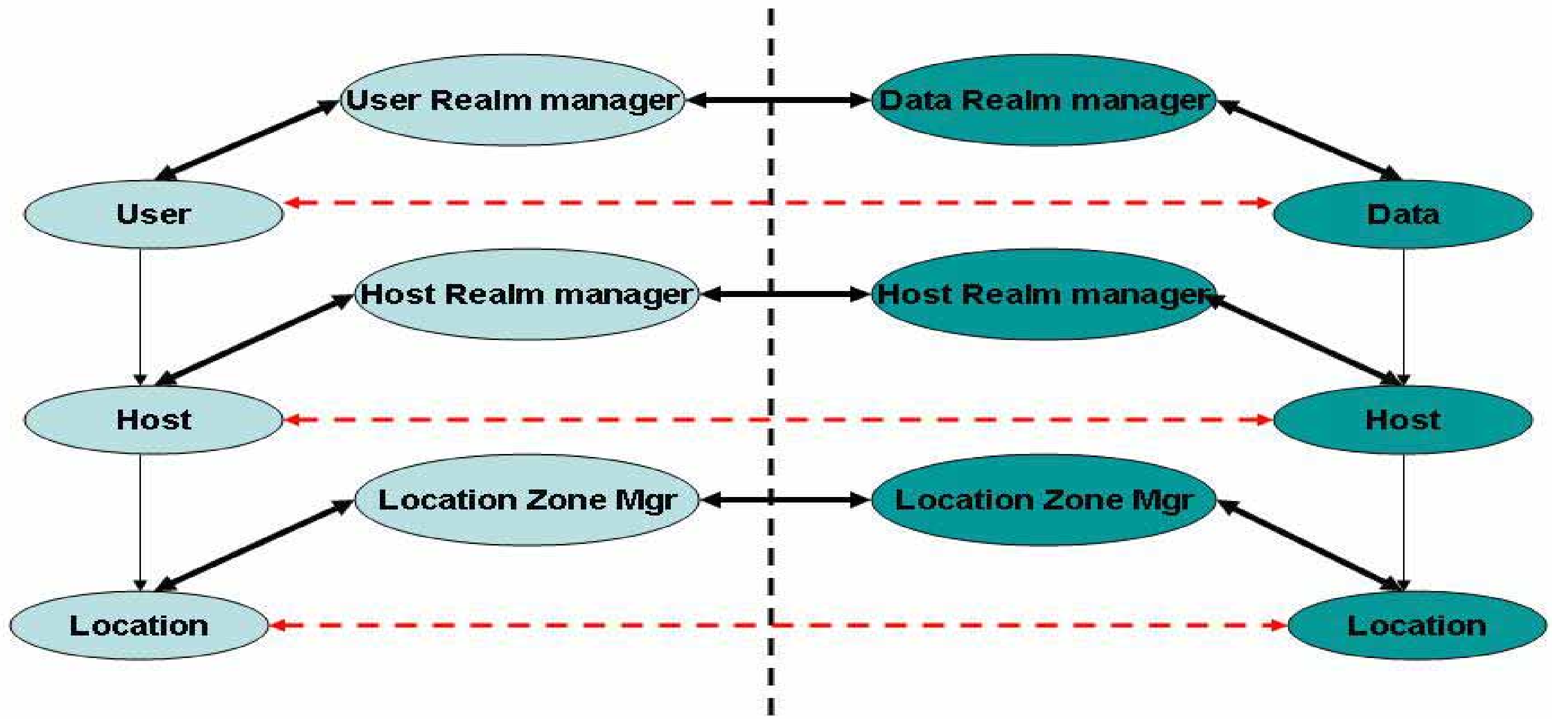
MILSA: Future Work

- Signaling messages and mechanism definition
- Location privacy
- NAT
- Traffic Engineering
- Multicast and Anycast
- Security:
  - Methods for quantifying trust
  - Protocol for disseminating trusted node's information
- Implement MILSA

User- Host- and Data Centric Models

- All discussion so far assumed host-centric communication
  - Host mobility and multihoming
  - Policies, services, and trust are related to hosts
- User Centric View:
  - Bob wants to watch a movie
  - Starts it on his media server
  - Continues on his iPod during commute to work
  - Movie exists on many servers
  - Bob may get it from different servers at different times or multiple servers at the same time
- Can we just give addresses to users and treat them as hosts? No! $\Rightarrow$ Policy Oriented Naming Architecture (PONA)

Policy Oriented Naming Architecture



- Both Users and data need hosts for communication
- Most communication is user-data communication
- Data is easily replicable and any copy is as good as any other
- Users have to follow organizational policies and data access policies are set by data owner.

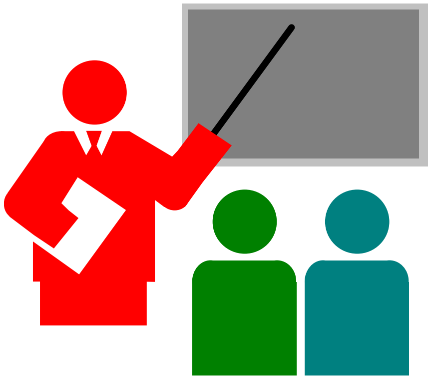
PONA (Cont)

- User and data realms are higher layer than host realms
  - Hosts move from one address to next
  - Users and data can move from one host to the next
- User realm manager keeps track of User's host ID(s) and enforces organizational policies about which hosts and data that user can access
- Data realm manager keeps track of data's host ID(s) and enforces policies about which hosts can the data reside on and which user can access it
- User realm manager (RZBS) translates user IDs to Host IDs. Host real manager translates host ID to address.
  $\Rightarrow$ Allows user, host, data mobility

PONA: Additional Benefits

- NAT Traversal
- Generic transfer layer
- Application Specific Transfer Layers
- Delay Tolerant Networking

Summary



1. Key Problems for next-gen Internet: Security, Mobility, and energy efficiency. Solution: Internet 3.0
2. MILSA allows mobility, multihoming, and enforces trust policies.
3. Separate logical relationships (realms) from Physical connectivity (zone).
4. Separate control and data planes, Hierarchical URI-like IDs, Realm-Zone bridging server
5. Policy oriented naming architecture (PONA) for User-centric and data-centric communication.

References

1. Jain, R., "Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation," in Proceedings of Military Communications Conference (MILCOM 2006), Washington, DC, October 23-25, 2006.
2. Jianli Pan, Subharthi Paul, Raj Jain, and Mic Bowman, "MILSA: A Mobility and Multihoming Supporting Identifier-Locator Split Architecture for Naming in the Next Generation Internet,," submitted to Globecom 2008.
3. Subharthi Paul, Jianli Pan, Raj Jain, "A Survey of Naming Systems: Classification and Analysis of the Current Schemes Using a New Naming Reference Model," to be submitted for publication, 2008.