MobilityFirst: A Robust and Trustworthy Mobility-Centric Architecture for the Future Internet
PIMRC Keynote, Sept 13, 2011

Contact: D. Raychaudhuri
WINLAB, Rutgers University
Technology Centre of NJ
671 Route 1, North Brunswick,
NJ 08902, USA
ray@winlab.rutgers.edu
MobilityFirst Project: Collaborating Institutions

D. Raychaudhuri, M. Gruteser, W. Trappe, R. Martin, Y. Zhang, I. Seskar, K. Nagaraja, S. Nelson

A. Venkataramani, J. Kurose, D. Towsley

S. Bannerjee

W. Lehr

X. Yang, R. RoyChowdhury

G. Chen

M. Reiter

Z. Morley Mao

B. Ramamurthy

Project Funded by the US National Science Foundation (NSF)
Under the Future Internet Architecture (FIA) Program, CISE

+ Also industrial R&D collaborations with AT&T Labs, Bell Labs, NTT DoCoMo, Toyota ITC, NEC, Ericsson and others.
Introduction
Vision: Mobility as *the* key driver for the future Internet

- Historic shift from PC’s to mobile computing and embedded devices…
  - ~4 B cell phones vs. ~1B PC’s in 2010
  - Mobile data growing exponentially – Cisco white paper predicts 3.6 Exabytes by 2014, significantly exceeding wired Internet traffic
  - Sensor/IoT/V2V just starting, ~5-10B units by 2020

![Diagram showing the transition from ~1B server/PC’s and ~700M smart phones in 2010 to ~2B servers/PC’s, ~10B notebooks, PDA’s, smart phones, sensors in 2020.](source)
Vision: Near-term “mobile Internet” usage scenario – cellular convergence

- ~4-5B new cellular devices in just a few years will drive convergence of technical standards and business models
  - Currently involves 2 sets of addresses (cellular number & IP), 2 sets of protocols (3GPP and IP), and protocol gateways (GGSN, PDN GW, etc.)
  - Scalability, performance and security problems when bridging 2 networks
  - Cross-layer interaction between PHY/MAC and TCP/IP impacts performance
  - Lack of a single unified standard inhibits mobile Internet app development across diverse networks and platforms
Vision: Near-term “mobile Internet” usage scenario – Mobile P2P and Infostations

- P2P and Infostations (DTN-like) modes for content delivery becoming mainstream
  - Heterogeneous access; network may be disconnected at times
  - Both terminal & network mobility; dynamic trust → identity vs. address
  - Requires content caching and opportunistic data delivery

MOBILE INTERNET

- Mobile DTN Router
- Roadway Sensors
- Opportunistic High-Speed Link (MB/s)
- Ad-Hoc Network
- Mobile P2P User
- Mobile DTN User/Router
- Infostations Router
- Disconnection
  - Opportunistic access
  - Message ferry/DTN
  - Content delivery/cache

WINLAB
Vision: Future “mobile Internet” usage scenarios – vehicular networks

- 100’s of million cars will be equipped with radios by ~2015
  - Both V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) modes
  - Involves capabilities such as location services, georouting, ad hoc networks
  - Important new trust (security and privacy) requirements in this scenario

Geographic routing/multicast
Dynamic network formation, trust
Location & context services
Vision: Emerging “mobile Internet” usage scenarios – pervasive/M2M/IoT

- The next generation of Internet applications will involve interfacing human beings with the physical world
  - Wide range of usage scenarios including healthcare, smart grids, etc.
  - Networking requires awareness of location, content and context
  - Challenges – content/context services, security and robustness
  - “Cloud computing” models with in-network processing & storage
Vision: Protocol Design for the future Mobile/Wireless World

- Fundamental change in design goals and assumptions
  - ~10B+ mobile/wireless end-points as “first-class” Internet devices
  - Mobility as the norm for end-points and access networks
  - Wireless access – varying link BW/quality, multiple radios, disconnections
  - Stronger security/trust/robustness requirements due to:
    - open radio medium
    - need for dynamic trust association for mobile devices/users/data/networks
    - increased privacy concerns (e.g. location tracking)
    - greater potential for network failure
  - Mobile applications involve location/content/context and energy constraints

- Technology has also changed a lot in the ~40 yrs since IP was designed
  - Moore’s law improvements in computing and storage (~5-6 orders-of-magnitude gain in cost performance since 1970)
  - Edge/core disparity, fast fiber but continuing shortage of radio spectrum
MobilityFirst is a clean-slate architecture that directly addresses these requirements while taking into account technology constraints and Moore’s Law advances.

Proposed network design highlights include:

- Separation of names & addresses for identity management (…no single root of trust)
- Global directory service for dynamic binding of identity with net address
- PKI names with unified framework for mobile devices, networks, content, context, ..
- Generalized delay tolerant network (GDTN) routing for efficiency and robustness in the presence of disconnection and access BW variation
- In-network storage and hop-by-hop transport of large data units
- Inter-network routing with enhanced flexibility and path choice
- Multicast, multipath, anycast as basic routing capabilities
- Content- and context-aware network services
- Optional computing layer for specialized services such as privacy or caching

Clean-slate architecture is a research methodology to identify useful protocol innovations – in practice, changes to network will be evolutionary.
Architecture Summary
Architecture: *MobilityFirst* Network Overview

- **MobilityFirst key protocol features:**
  - Separation of naming & addressing
  - Public-key globally unique identifier (GUID) and flat network address (NA)
  - Storage-aware (GDTN) routing
  - Multicast, multipath, anycast services
  - Flexible inter-domain boundaries and aggregation level
  - Early binding/late binding options
  - Hop-by-hop (segmented) transport
  - Support for content & context
  - Strong security and privacy model
  - Separate mgmt & computing layers

- Several new protocol components, very distinct from today’s TCP/IP ….
Architecture Concepts: Name-Address Separation

- Separation of names (ID) from network addresses (NA)
- Globally unique name (GUID) for network attached objects
  - User name, device ID, content, context, AS name, and so on
  - Multiple domain-specific naming services
- Global Name Resolution Service for GUID → NA mappings
- Hybrid GUID/NA approach
  - Both name/address headers in PDU
  - “Fast path” when NA is available
  - GUID resolution, late binding option
Architecture Concepts: Global Name Resolution Service for Dynamic Name <-> Address Binding

- Fast Global Name Resolution a central feature of architecture
  - GUID <-> network address (NA) mappings
- Distributed service, possibly hosted directly on routers
  - Fast updates ~50-100 ms to support dynamic mobility
  - Service can scale to ~10B names via P2P/DHT techniques, Moore’s law
Protocol Design: Direct Hash GNRS

- Fast GNRS implementation based on DHT between routers
  - GNRS entries (GUID <-> NA) stored at Router Addr = hash(GUID)
  - Results in distributed in-network directory with fast access (~100 ms)

### Global Prefix Table

<table>
<thead>
<tr>
<th>Prefix</th>
<th>AS #</th>
<th>Next-hop address</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/8</td>
<td>1</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>67.10/16</td>
<td>55</td>
<td>67.10.1.1</td>
</tr>
<tr>
<td>44/8</td>
<td>101</td>
<td>44.32.1.1</td>
</tr>
</tbody>
</table>

**Diagram**

- User A (GUID = 10) searches for User B (GUID = 10)
- Results in distributed in-network directory with fast access (~100 ms)

**Legend**
- Resolver/Router Update Flow Query Flow

**Internet Scale Simulation Results**

Using DIMES database
**Architecture Concepts: MobilityFirst**

Routing Design Goals

- Routing protocol should seamlessly support a wide range of usage scenarios, from wired → mobile → ad hoc → DTN
  - Device, content and network mobility
  - Heterogeneous devices and radio access
  - Robustness to varying BW, disconnection
  - Dynamic network formation & flexible boundaries
**Architecture Concepts: Exploiting In-Network Storage for Routing**

- Expands routing options
  - *Store* and/or *replicate* as feasible routing options
  - Enables “late binding” routing algorithms
- Hop-by-hop transport
  - Large *blocks* reliably transferred at link layer
  - Entire block can be stored or cached at each router

**Generalized Storage-Aware Routing**

- Actively monitor link qualities of network
- Router store or forward decision based on:
  1. Short and long term link qualities
  2. Available storage along path
  3. Connectivity to destination

**Take advantage of cheap storage in the network (storage-aware routing)**

- ~100MB, data in transit
- ~10GB, in-network storage
- ~1TB, content caching
Protocol Design: Storage-Aware Routing (GSTAR)

- Storage aware (CNF, generalized DTN) routing exploits in-network storage to deal with varying link quality and disconnection.
- Routing algorithm adapts seamlessly from switching (good path) to store-and-forward (poor link BW/short disconnection) to DTN (longer disconnections).
- Storage has benefits for wired networks as well.
Protocol Design: Segmented Transport

- Segment-by-segment transport between routers with storage, in contrast to end-to-end TCP used today.
- Unit of transport (PDU) is a content file or max size fragment.
- Hop TP provides improved throughput for time-varying wireless links, and also helps deal with disconnections.
- Also supports content caching, location services, etc.
Architecture Concepts: MobilityFirst
Interdomain Routing

- Requirements include: flexible network boundaries, dynamic formation, virtual nets, network mobility, DTN mode, support for path selection, multipath, multi-homing, improved security, etc.
- Motivates rethinking of today’s 2-tier IP/BGP architecture (inter-AS, intranet)
- MobilityFirst interdomain approach uses GNRS service + enhanced path vector routing to achieve design goals – still evaluating multiple design options….
Protocol Design: MobilityFirst Interdomain Routing

- One approach under consideration is to enhance BGP-like protocols with summary node/link info (“Vnode graph”)
  - Summary knowledge of access net properties (Mbps, % avail, etc.), ingress/egress points and alternate paths exchanged between networks/AS’s
  - Network topology information for identifying multiple paths, storage points, etc.

- Inspired by “Vnode” concept in “Pathlet” routing (Godfrey, 2008)

- Support for multicast, anycast, multihoming and multipath

![Diagram of network topology with Vnode properties and path information](image-url)
Protocol Design: Virtual Routing Domains

- Virtual network domains can be created by combining Vnodes and/or networks into logical aggregates
  - Vnodes and networks can form VN’s without having to be physically contiguous – GNRS provides membership list & trust relationships
  - Virtual networks share fine-grain intra-domain routing information & expose multiple ingress and egress points to the inter-domain protocol
  - Can be used to aggregate disjoint wireless access networks (e.g. “NJfreeWiFi”) or set up a “mobile cloud service” with improved routing visibility; many other uses ….
Protocol Design: Content Delivery in MobilityFirst

- Content delivery handled efficiently by proposed MF architecture
  - “Content objects” identified by unique GUID
  - Multiple instances of content file identified by GNRS via GUID to NA mapping
  - Routing protocol used for “reverse anycast” to nearest content object

- Approach differs from NDN/CCN, where content attributes are carried in packet headers

- MF uses content GUID naming service & GNRS to keep things general and avoid interpreting content semantics inside network
Protocol Design: Context Aware Delivery

- Context-aware network services supported by MF architecture
  - Dynamic mapping of structured context or content label by global name service
  - Context attributes include location, time, person/group, network state
  - Context naming service provides multicast GUID – mapped to NA by GNRS
  - Similar to mechanism used to handle named content

Context = geo-coordinates & first_responder

Send (context, data)
Protocol Design: Management Plane

- Separate mgmt plane designed into MF architecture
  - Provides visibility into key mobile network aspects such as name resolution, disconnected operation, wireless access quality, context-aware services, location, privacy, …
  - Includes mechanism for network-assisted dynamic spectrum assignment (DSA) as a basic capability
  - Intended to improve transparency and support add-on mgmt services
Protocol Design: Management Plane (cont.)

- Support for dynamic spectrum assignment (DSA)
  - Given that the majority of end-user devices are wireless, Internet spectrum should be assigned on demand
  - Management plane mechanism for exchange of spectrum use data

![Diagram of spectrum management and control](image)

- Distributed Spectrum Coordination Algorithm Software (runs on all radio devices)
- Radio Coverage: Region A, Region B, Region C, Region D
- Geo-cast Spectrum Update Service
- Mobility First Control & Management Plane
- Aggregate Spectrum Updates Between Routers
- Spectrum Use Update (from Radios)
- Spectrum Occupancy Map (from Routers)
Protocol Design: Computing Layer

- Programmable computing layer provides service flexibility and evolution/growth path
  - Routers include a virtual computing layer to support new network services
  - Packets carry service tags and are directed to optional services where applicable
  - Programming API for service creation provided as integral part of architecture
  - Computing load can be reasonable with per-file (PDU) operations (vs. per packet)
Protocol Design: Packet Headers and Forwarding with Hybrid GIUD/NetAddr

- Hybrid scheme in which packet headers contain both the object name (GUID) and topological address (NA) routing
- NA header used for “fast” path, with fallback to GUID resolution where needed
- Enables flexibility for multicast, anycast and other late binding services

<table>
<thead>
<tr>
<th>Name</th>
<th>GUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>server@winlab</td>
<td>xy17519bbd</td>
</tr>
</tbody>
</table>

GUID/Service Header Components

- Optional list of NA’s
  - Destination NA
  - Source route
  - Intermediate NA
  - Partial source route

GUID with GUID Header only

PDU with GUID and NA headers

Routing Table

<table>
<thead>
<tr>
<th>Dest NA</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net 123</td>
<td>Net11, net2,..</td>
</tr>
</tbody>
</table>

GUID/Service Header

GUID Address Mapping

<table>
<thead>
<tr>
<th>GUID</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>xz1756..</td>
<td>Net 1194</td>
</tr>
</tbody>
</table>

Net 1194

GUID/Public Key Hash

SID (Service Identifier)

Network Address Based Routing (fast path)
Use Cases: GUID/Address Routing
Scenarios – Dual Homing

- The combination of GUID and network address helps to support new mobility related services including multi-homing, anycast, DTN, context, location …
- Dual-homing scenario below allows for multiple NA:PA’s per name
Use Cases: GUID/Address Routing Scenarios – Handling Disconnection

- Intermittent disconnection scenario below uses GUID based redirection (late binding) by router to new point of attachment.

Guidance:
- Send data file to “Alice’s laptop”

GUID/SID: NA1.PA7

Current network address provided by GNRS;
NA1 – network part; PA7 – port address

GUID: NA7.PA3

Successful redelivery after connection

DATA

PDU Stored in router - GUID resolution for redirection

GUID

NetAddr= NA1.PA9 - Delivery failure

Data Plane

Mobility Trajectory

Disconnected Region
Use Cases: GUID/Address Routing
Scenarios – Multicast/Anycast/Geocast

- Multicast scenario below also uses GUID <-> Network Address resolution (late-binding) at a router closer to destination (..GUID tunnel)

GUID/SID
Send data file to “WINLAB students”

Intermediate network address NA1 provided by GNRS

GUID
NetAddr=NA1:PA1,PA2,PA9; NA7,PA22

GUID <-> addr
Binding at NA1

Late GUID <-> addr
Binding at NA1

Port 1
NetAddr=NA1,PA1

Port 2
NetAddr=NA1,PA2

Port 22
NetAddr=NA7,PA22
Security Considerations:

- Public keys names for hosts & networks; forms basis for
  - Ensuring accountability of traffic
  - Ubiquitous access-control infrastructure
  - Secure routing; no address hijacking

- Emphasis on achieving robust performance under network stress or failure
  - Byzantine fault tolerance as a goal
  - Transform malicious attacks into benign failure
  - Performance observability (in management plane)

- Intentional receipt policies at networks and end-user nodes
  - Every MF node can revert to GUID level to check authenticity, add filters, ...

- No globally trusted root for naming or addressing
  - Opens naming to innovation to combat naming-related abuses
  - Removes obstacles to adoption of secure routing protocols
Security Considerations: Trust Model

- Secure Host Name Service Lookup
- Secure GNRS Update
- Secure InterNetwork Routing Protocol
- Secure Data Path Protocol
- GUID = public Key
- GUID <-> NA binding
- Aggregate NA166: NA14, NA88, NA33
- NA14, NA88, NA33
- Public Key object and network names enable us to build secure protocols for each interface shown

Name assignment & certification services (can incorporate various kinds of trust including CA, group membership, reputation, etc)
Privacy Considerations:

- Public keys as addresses enable their use as pseudonyms
  - Can be changed frequently by end-users to interfere with profiling
  - Flat-label PKI addresses provide an additional layer of routing privacy

- Openness in naming & addressing introduces competition on grounds of privacy
  - E.g., enable retrieval of mappings in a privacy-preserving way

- Virtual service provider framework can optionally provide enhanced support for privacy
  - E.g., constant-rate traffic between routers to defeat traffic analysis

- Route transparency and selection supports user choice on privacy grounds
Prototyping & Evaluation
MobilityFirst Prototyping: Phased Approach

Evaluation Platform

- Standalone Components
- System Integration
- Deployment ready

Prototyping Status

Simulation/Emulation
Emulation/Limited Testbed
Testbed/‘Live’ Deployment

- Context Addressing Stack
- Content Addressing Stack
- Host/Device Addressing Stack
- Encoding/Certifying Layer
- Global Name Resolution Service (GNRS)
- Storage Aware Routing
- Locator-X Routing (e.g., GUID-based)
- Context-Aware / Late-bind Routing
- Encoding/Certifying Layer
- Global Name Resolution Service (GNRS)
- Storage Aware Routing
- Context-Aware / Late-bind Routing
- Locator-X Routing (e.g., GUID-based)
- IP Routing (DNS, BGP, IGP)
MobilityFirst Prototyping: ORBIT Grid & WiMax Testbeds for Wireless Edge Evaluation

- Multi-radio indoor and outdoor nodes - WiMAX, WiFi,
- Linux-based Click implementation of routing protocols
MobilityFirst Prototyping: Software Router

- Linux-based software router with two-level implementation

![Diagram of MobilityFirst Prototyping: Software Router]

- User-Level Control Plane
  - MF App Services
  - MF Name Resolution
  - MF Routing & Mgmt.

- Portable user-level implementation

- OpenFlow Controller
  - XORP
  - Quagga

- Forwarding Engine
  - Linux routing
  - Click
  - Commodity Hardware
  - NetFPGA
MobilityFirst Prototyping: Android Client

- **Device:** HTC Evo, Android 2.3
  - Unbranded and rooted
  - Development: SDK, NDK, flash a modified kernel (if required)
  - WiFi, WiMAX interfaces

- **Modules in Android’s MF stack**
  - MF-socket API - user level library
  - Transport layer
  - Storage aware routing
  - SHIM layer support for multi-homing
  - 1-Hop reliable data transfer

- **MF-socket API**
  - open, send, send_to, recv, recv_from
  - User policies for resource use and intentional data receipt
MobilityFirst Prototyping: GENI Deployment Plan (Phase 3)

Legend
- Internet 2
- National Lambda Rail
- OpenFlow Backbones
- OpenFlow
- WiMAX
- ShadowNet

Mapping onto GENI Infrastructure
ProtoGENI nodes, OpenFlow switches, GENI Racks, WiMAX/outdoor ORBIT nodes, DieselNet bus, etc.

Deployment Target:
- Large scale, multi-site
- Mobility centric
- Realistic, live
MobilityFirst Prototype: Multi-Site GENI Demo (GEC12, ~4Q2011)

- Edge networks NA-1, NA-2 connected to global core
- Each of NA-1, NA-2 are contained MF routing domains
- Each WiMAX BSS and WiFi AP is associated with a MF Router
- Node a is multi-homed within a network
- Node c is multi-homed across 2 networks

![Diagram of MobilityFirst Prototype](image)

- WiFi AP
- WiMAX BSS
- MF Router
- Android Client w/ WiMAX + WiFi
- Linux PC/laptop w/ WiMAX + WiFi
- Vehicular node w/ WiMAX
- Sensor node
- MF Sensor GW
- GENI Core
- Campus Network (at Rutgers)
- Campus Network (at other GENI site)
Resources

- Project website: [http://mobilityfirst.rutgers.edu](http://mobilityfirst.rutgers.edu)

- GENI website: [www.geni.net](http://www.geni.net)