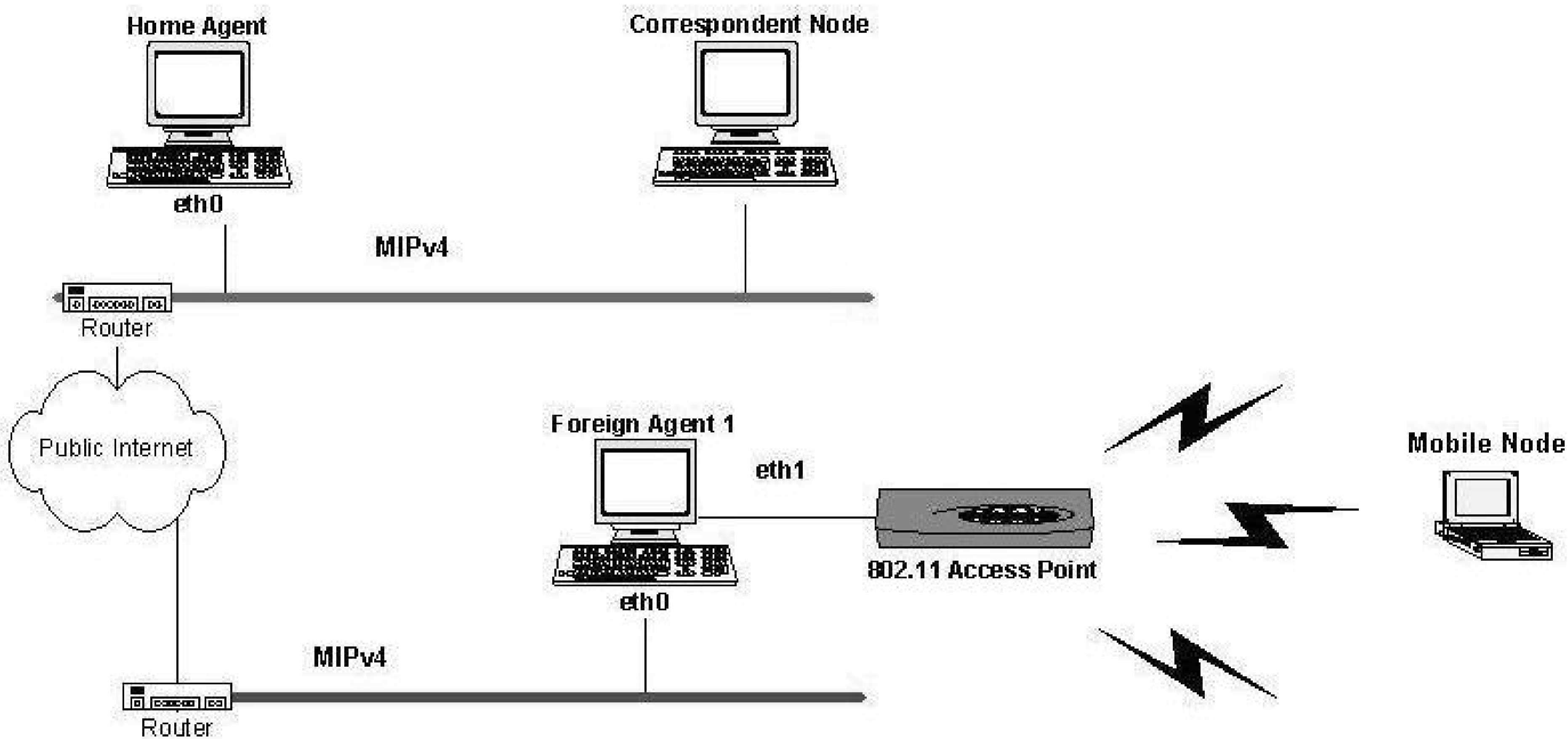
Efficient IP-Based UMTS Networks

Joseph Thomas *and* Lan Luo
University of Maryland, Baltimore County

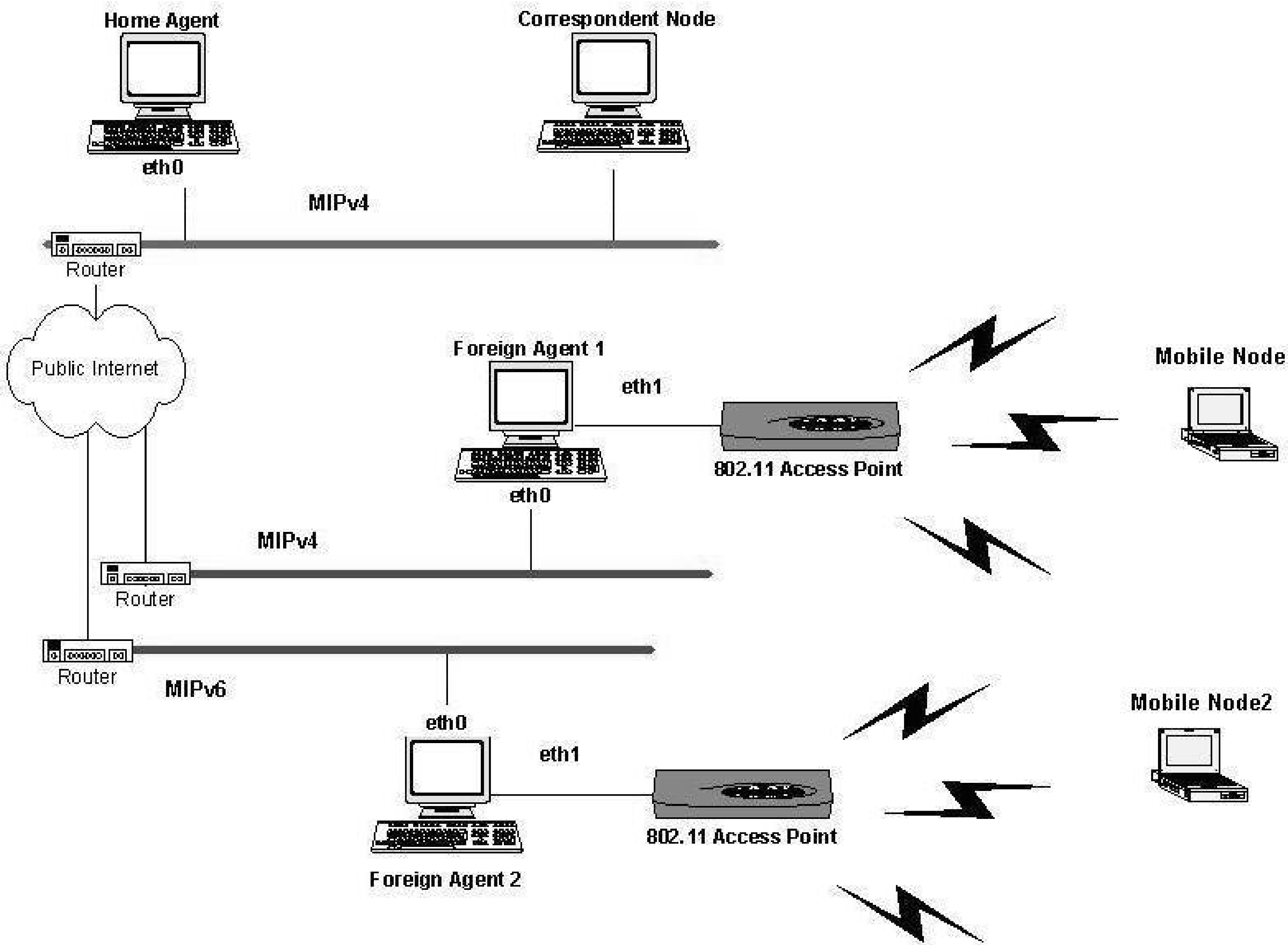
Objectives

- Functionality, Security, and Connectivity Tests in MIPv4 and v6 networks
- MIPv4: Mobile Node (MN), Home Agent (HA), Foreign Agent (FA), Correspondent Node (CN); Care-of addresses (CoA); Tunneling
- MIPv6: Address space expansion; No FA; CoA autoconfiguration; Route discovery; Router-assisted smooth handoff; Security as in IPv6

UMBC Testbed



Extended Testbed



Experiments – Phase I
(in cooperation with BBN Technologies)

- Hand-off between networks *(delays)*
- Security Association between MN and HA *(Shared Key, SPI, Encryption)*
- Redirection *(potential denial-of-service)*
- Replay Protection *(timestamp)*

Phase II: Authentication of FA

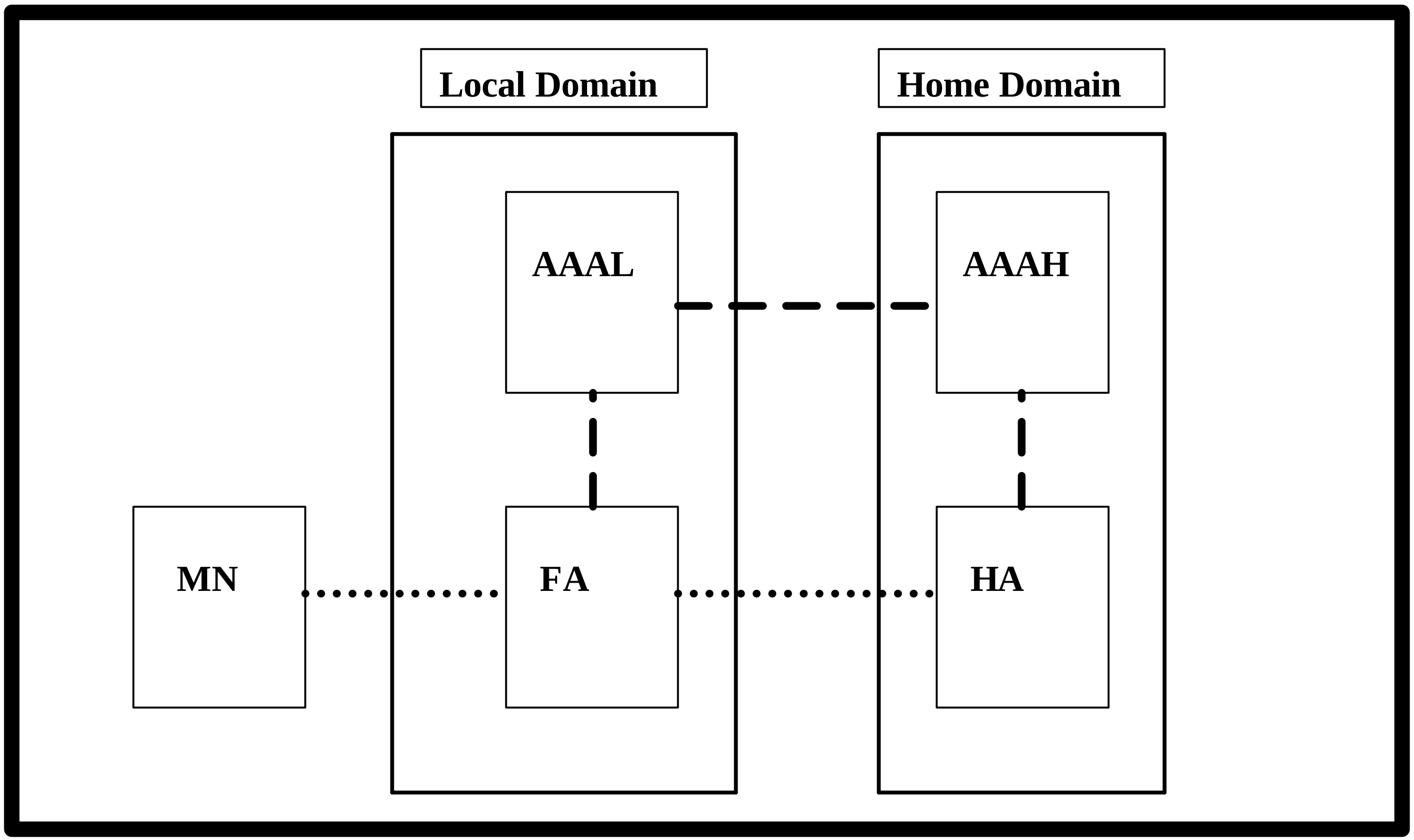
- Authentication via key distribution (RFC 3344)
  - N! (i.e., approx. N^N) secret keys
  - Practical difficulties
- Prevention of service-denial attacks
- Need for reliable billing procedures
- Two approaches
  - Public key certificate protocol
  - MIP with Authorization, Authentication, and Accounting (AAA)

Public Key Certificate Protocol

- Each mobile agent holds a public key and a private key, and receives the services of a trusted third party called a Certificate Agent (CA)
  - 2^N keys rather than N^N keys
- CAs are centralized: problems from failures and bottlenecks
- A trust-hierarchy path of CAs

MIP with AAA

- Each domain has a AAA server
- Security relationships between mobile agent, its home AAA (AAAH) server, and its local AAA (AAAL) server
- Tasks of AAA server
  - Initiate/enable the authentication for MIP registration
  - Authorize MN to use MIP and certain specific services
  - Initiate accounting for service utilization



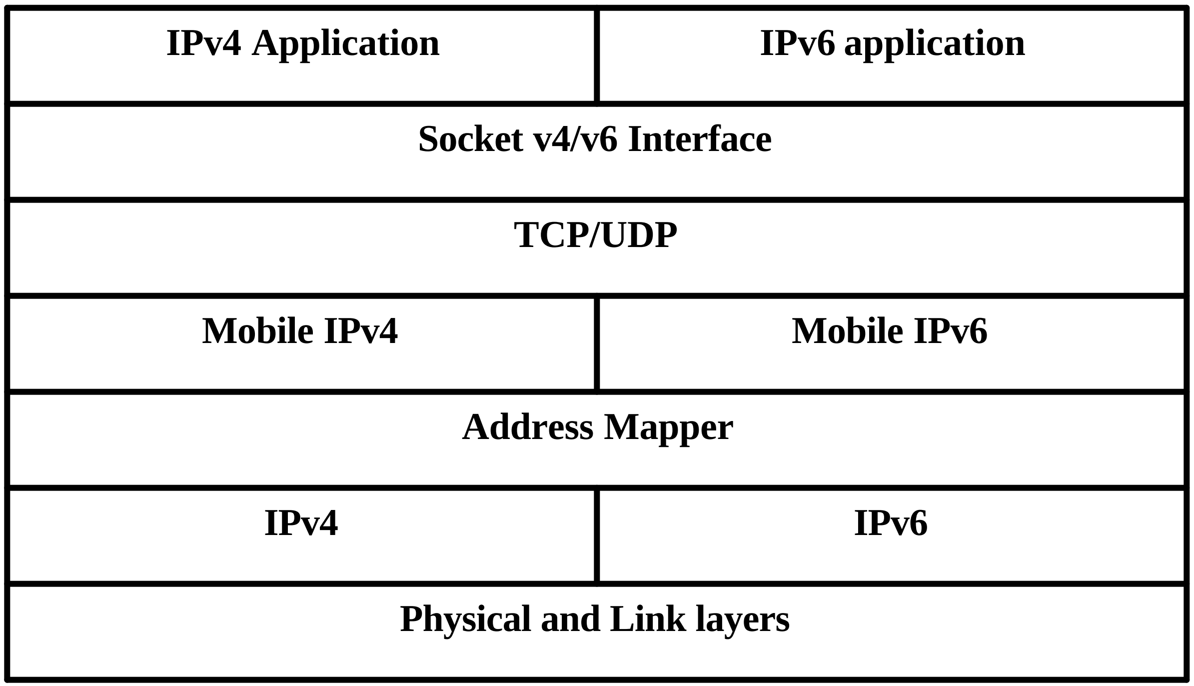
AAA Servers with Mobile IP

Security of Data Transmission in MIP v4

- In MIPv4, messages are authenticated but not encrypted
  - Wireless links are vulnerable to attack despite WEP (e.g., Ethereal, Airsnort)
  - Integrate IPSec with Mobile IP
- IPSec: Essentially encrypts packets at IP layer; provides authentication, access control, and replay protection
- Transport mode, Tunnel mode, or Security gateway

Interconnectivity of MIPv4 and MIPv6 Networks

- No FAs in MIPv6: CoAs autoconfigured by MNs
  - An MIPv4 MN in an IPv6 network is unhappy!
  - Likewise for an MIPv6-MN in an IPv4 network (no CoA)
- Dual Stack Implementations with address mapper
  - Detect movements between different IP version networks
  - Associate CoA of one IP version network with another I
  - Receive/forward MIP messages in different IP versions
  - Dispatch IPv4/IPv6 packets and MIPv4/v6 messages to the correct upper layers transparently



Dual stack Architecture

Dual Stack MN, HA Operations

- IPv6 home network, IPv4 foreign network:

  MN registers an IPv6 home address; receives agent advertisement from MIPv4 FA via IPv4 protocol stack; obtains an IPv4 CoA from FA and generates the IPv4-compatabile IPv6 address; obtains IPv4 address of its HA; tunnels MIPv6 registration messages to its HA via IPv4 stack

- IPv4 home network, IPv6 foreign network:

  MN registers an IPv4 home address; receives router advertisement from IPv6 router via Ipv6 protocol stack; autoconfigures an IPv6 COA and maps it to an IPv4 version; obtains an IPv6 address for its HA; tunnels MIPv4 registration message to MN's HA in IPv6 packets

Conclusions

- Planned experiments will take-off when UMBC receives its IPv6 connection (mid-July)
- Other related research:
  - Cooperative networks and distributed multiplexing
  - Data compression for sensor network nodes
  - Capacity bounds for sensor networks …