Networks and Mobile Systems

overview	-	Elevator pitch
projects	-	Projects
people	-	Who are we?
publications	-	NMS Papers
software	-	Software and hardware releases from the NMS group
support	-	Who sponsors NMS?

Overview

The NMS group at MIT's Computer Science and Artificial Intelligence Laboratory conducts research in many areas of networking: wireless networks, Internet architecture and protocols, overlay and peer-to-peer networks, sensor networks, network security, and networked systems. The group was formed in 1998.

Current projects

- Datacenter networks and cloud infrastructure
  - Fastpass and Flowtune
  - Domino: programmable router data planes
  - Flexplane: whole-network emulation in software for programmability
- Mobile and sensor computing
  - Glimpse: a continuous object recognition system
- Transport protocols and mechanisms
  - Remy (TCP ex machina, computer-synthesized congestion control)
  - Mahimahi (record-and-replay framework for web traffic)

Unfortunately, the above list might be a bit out-of-date. The NMS papers page has a more current list of papers.

Some past projects

Internet architecture, overlay and P2P networks

P2P and overlay networks

- **Chord**: a scalable and robust distributed hash table (DHT) enabling key-value lookups.
- **Project IRIS**: A multi-institution NSF ITR collaboration that developed the network and system infrastructure for resilient Internet services using DHTs. Our work included:
  - **Dynamic evolution of P2P systems**: The amount of work required to maintain good connectivity depends on the "half-life" of a P2P system.
  - **SFR** (Semantic-Free Referencing), a reference (name) resolution service for linked systems.
  - **DOA** (Delegation-Oriented Architecture), an extension to the Internet architecture that accommodates "middleboxes" in an architecturally coherent way using a new *delegation* primitive.
  - **DQE** (Distributed Quota Enforcement), a spam control system.
  - **Speak-up**, a defense against application-level DDoS attacks.
- **RON** (Resilient Overlay Networks): Improving availability and resilience of Internet paths using application-controlled overlay routing.
- **MONET**: Multi-homed overlay network of web proxies to route around network failures for Web applications.

Congestion control, traffic engineering

- **XCP** (eXplicit Congestion Control) and **TeXCP**: Congestion control for high bandwidth-delay product networks and responsive traffic engineering.
- **CM** (Congestion Manager), an integrated end-to-end congestion management architecture and congestion control algorithms for the

Internet routing

- **rcc** and correct Internet routing: tools to improve routing correctness and experimental studies of Internet routing and failures.
- **R-BGP**: Improving Internet routing connectivity.
- **BGPSep:** Constructing correct and scalable iBGP configurations.

Network measurement

- **DNS analysis**: trace-based analysis of DNS performance and caching.
- **M&M tools:** multiQ and mystery, passive measurement tools suitable for large scale studies of Internet path characteristics
- **Routing analysis**: BGP measurements.

Wireless, mobile, and sensor networks

- **CarTel**: a mobile sensor network system developing vehicular network protocols, software, and services.
- **Cricket**: An accurate indoor location system. (Now commercially available.)
- **SoftPHY and its applications**: using cross-layer confidence information (SoftPHY) from the physical layer to design better higher-layer wireless network protocols.
- **INS** is an *intentional naming system* for scalable and dynamic resource discovery. **Twine** aims to make INS scalable to large networks using peer-to-peer lookups, built on top of **Chord**.
- **Migrate**, an end-to-end architecture for Internet host mobility, support for suspend/resume operations for mobile network applications to handle disconnections, and server failover.
- *Harnessing multiple radios and access points*
    - **FatVAP:** Aggregating AP backhaul bandwidth.
    - **Horde**: networking software that allows an application to stripe data from multiple streams across a set of dissimilar wireless network channels.
    - **Divert**: a multi-radio, fine-grained path selection system for improving throughput in wireless LANs.
    - **APware**: improving performance and robustness for multi-rate wireless LANs.
- **Fusion:** Mitigating congestion in wireless sensor networks.
- **BSD** (**Bounded SlowDown**), **Span**, **LEACH** and **Spin**: energy-efficient protocols for wireless and sensor networks
- **Spectrumware**: new algorithms for radio and wireless physical layers for implementation on a flexible software platform. (Now commercially available.)
- **Blueware**, protocols for internetworking with Bluetooth.

Network security

- **AIP (Accountable Internet Protocol)**: self-certifying Internet addresses + new protocols to provide accountability and improve Internet security.
- **Kill-Bots**: Surviving application-layer botnet attacks that mimic flash crowds.
- **Real-Time anomaly detection**: Improving network security with real-time scanning and worm detection.
- **Speak-up**, a defense against application-level DDoS attacks using bandwidth as a "currency".
- **DQE** (Distributed Quota Enforcement), a spam control system.
- **Securing SSH** from address harvesting attacks.
- **Infranet**: circumventing Web censorship and surveillance.
- **RoboNorm:** Efficient and robust TCP stream normalization.

Distributed data management, stream processing

- **Medusa:** Distributed data stream processing.
- **HRDB**: Database fault-tolerance with heterogeneous replication.