

Main Theme: Diffuse Computing

Managing and maintaining a computational infrastructure, distributed among many heterogeneous nodes that do not trust each other completely and may have incentives (needs, priorities).

SPYCE Objective: Scaleable High Assurance



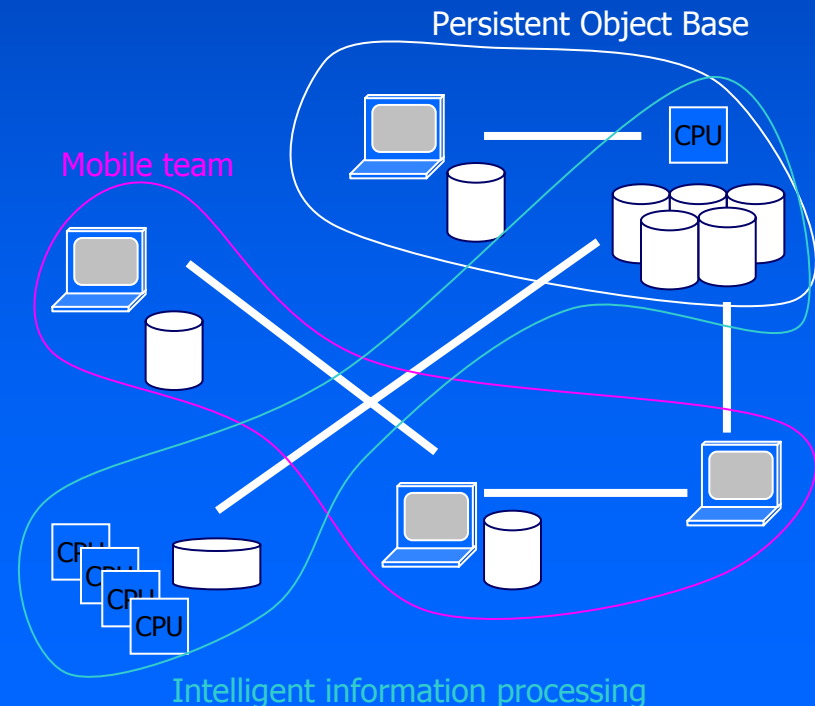
Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

Efficient Diffuse Multimedia Networking

Incentive Compatibility

Authorization Schemes

Secure Data Storage and Communication

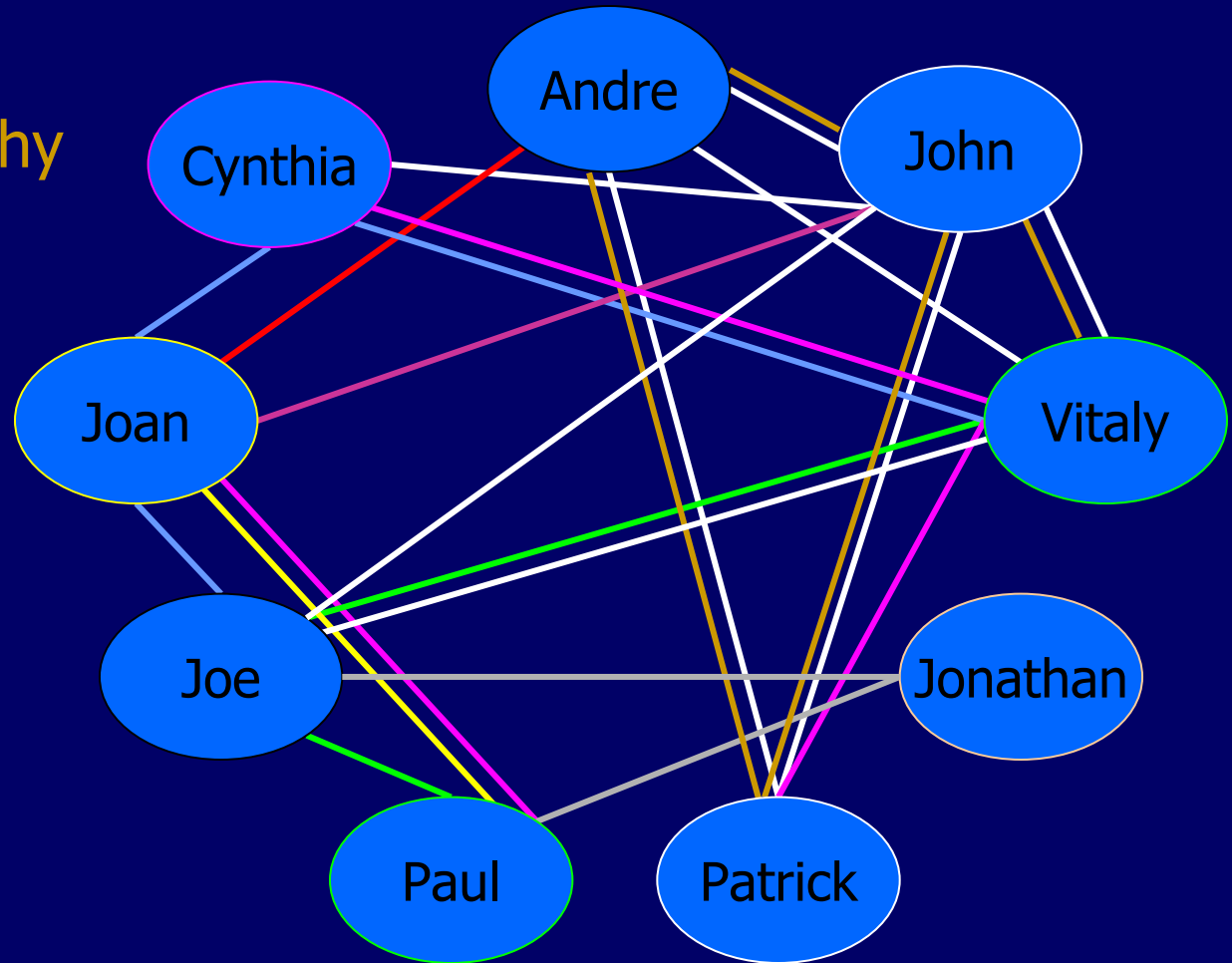


Presentations today

- Market-based computation (incentive-compatibility) Feigenbaum
- Communication and security protocols analysis Halpern
- Authorization mechanisms (trust management) Mitchell
- Privacy and anonymity Lincoln
- Networking Smith
- Poster Session

Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design
- Authorization
- Decision Theory
- BGP
- Digital Rights



Challenges Ahead

- Secure, reliable network infrastructure
 - Combine security mechanism and incentives
 - Examples: BGP, DNS, NTP, ...
- General theory of computational mechanism
 - Mechanism specification and verification
 - Computational complexity analysis combining network communication and incentives
- Discrete information management
 - Multicentric information delivery and retrieval
 - Access control, anonymity, and privacy

Summary of Project: Multidisciplinary Research

- Software Quality and Infrastructure Protection for Diffuse Computing
- Algorithms to model diffuse computing and achieve scaleable high assurance
- Multi-institution experimental platform





FY2001 ONR CIP/SW URI



Software Quality and Infrastructure Protection for Diffuse Computing



Principal Investigator: Andre Scedrov
Institution: University of Pennsylvania
URL: <http://www.cis.upenn.edu/spyce>

STARTED IN MAY 2001

