



Future Challenges in Networking Research

Panel Session at
**International Conference on Computer
Communications and Networks**
Oct 15, 2002

Dr. Mohammed Atiquzzaman
University of Oklahoma
Norman, OK 73019-6151, USA.
atiq@ou.edu
www.cs.ou.edu/~atiq



Growing Research Areas

- Ubiquitous computing and communications
 - Anywhere, anytime, anyone, anyhow, any.....
 - Application adaptability to anywhere, anytime,
- Optical Networking
 - Higher bandwidth allows future advanced and bandwidth hungry applications.
- Wireless and Mobile Networking
 - Anytime, anywhere network connectivity.
 - Horizontal and vertical handovers
 - Seamless roaming
 - High bandwidth → increase spectral efficiencies
- Network Security
 - security, privacy
- Adhoc Networking
 - Multihop networks, Power ...



Growing Research Areas (contd.)

- Highly distributed collaborative networks
 - Sharing of large amounts of data by scientists and researchers at geographically distributed locations all over the world
 - Instruments (astronomy, earthquake, observatories, etc.) may be distributed all over the world → high speed network required for this collaborative community
 - Sensor webs
 - Sensors collect data and share the information with other sensors
 - Applications in space research and military



Network Security

- **Trust**: security and privacy
- Increased emphasis on network security
 - Cyber-security is one of the top priorities on the Office of Homeland Security
- Network **monitoring** to signal impending attack
- Cybersecurity technologies and methods to develop advanced networks that can replace the vulnerabilities of today's Internet with **self-healing, trusted**, high-bandwidth systems for secure commerce, communication, and connectivity



Internet scalability/stability

- Large number of sensors in ad hoc mode generating large amounts of data
 - Sensor web, Distributed sensors
- Large number of researchers all over the world sharing large volume of data (observatories, weather, seismic)
- Example: Every person, in a football stadium with 100,000 people, has 100 nodes (PAN) => 10,000,000 nodes in a small area !!!
- Ultra-high speed networks



Securing the Cyberspace

- **Anyone** having access to Internet anywhere in the world has access to the US Internet
- Government, industry, commerce, financial institutions rely heavily on the **Internet**.
 - Energy, finance and banking, information and telecom, public health, emergency services, water, agriculture, postal services



Strategies in securing the cyberspace

- Deploy **threat management** tools to preempt attacks
- Continuously **check for unauthorized access** to wireless networks
- **Threat analysis** and **warning** capability
 - Detect incidents early
- **Respond quickly** in the case of attacks
 - Rapid response could stop the tide of an ongoing attack
- Develop **Secure IT** products
 - Security research
 - **Software development practices** to take security into account
 - Developing improved capabilities for **detecting malicious code**.
 - Federal **purchasing standards** to insist on security



Securing cyberspace (contd.)

- Cyber security is a **shared responsibility**.
 - No single industry is responsible for its security
 - No government entity can protect it
- Network **infrastructure protection**
- Internet was built with redundancy in mind, **NOT security**.



Example: Disaster Recovery

- **First responders** could not get access to telecommunication services during the 9/11 rescue operation
- Ensure that first responders have access to telecommunication and cyber access
 - **Reserve resources** for first responders - both computer and telecommunication networks
 - **Give priority** to first responders



References

- "Final Report on the Inter-Agency Workshop on Research Issues for Smart Environments", IEEE Personal Communications, Oct 2000.
- "Future Generation Wireless Networks", IEEE Personal Communications, Oct 2001.
- "Wireless Communications", IEEE Communications Magazine, May 2002.
- Various U.S. Government Documents, 2002.
- "The sensor Web: A new instrument concept", JPL, NASA.