

RESEARCH BRIEF

MULTIPOINT COMMUNICATION NETWORKS AND AD HOC NETWORKS

The potential

High performance fixed and/or mobile point-to-multipoint or multipoint to multipoint communications among sensors, robots and spacecraft has the potential for greatly increasing efficiency and security for commercial, military and NASA networks.

The challenge

The major challenge is to efficiently design networks and their high-quality protocols, such as routing, MAC, congestion and flow control and security. There is also a need to develop efficient methods of data dissemination and reliable and secure multicast for mobile ad hoc networks (MANETs).

The research

Researchers at ISR's Center for Satellite and Hybrid Communication Networks (CSHCN) have developed a novel multicast routing scheme for MANETs that creates a source-based mesh of nodes called "the flooding group" to distribute data. This on-demand protocol is created based on hop count distance constraints, which alleviates MAC problems. The nodes learn hop count metrics during the request-response phase. The scheme uses soft state group membership information. This probabilistic data forwarding mechanism improves efficiency. The researchers' primary scheme, PSP-SGFP, achieves a goodput of 85 to 90 percent, which is 5 to 8 percent lower than flooding. The efficiency improvement is between 20 and 40 percent.

A more realistic "hybrid automation" model has been developed for TCP over mobile wireless networks. This model captures the slow-start phase of TCP.

The researchers have also developed, implemented and tested a new swarm intelligence-based routing algorithm for MANETs. This algorithm is inherently scalable, resulting in graceful builds and degradations.

The researchers used change detection techniques and algorithms to develop new schemes for distributed detection of self-propagating code spreading, and distributed denial of service attacks.

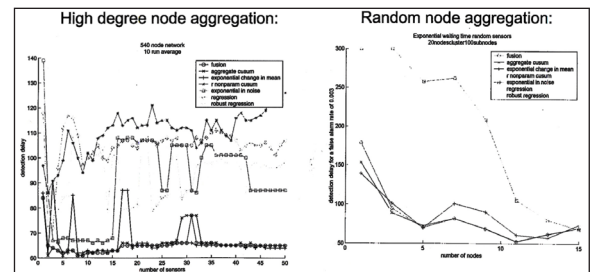
For MANETs, the researchers have developed and evaluated the performance of new schemes for detecting routing attacks, including routing table falsification and worm-hole attacks. They also have developed new key management

schemes for group communications, new

source authentication schemes for multicast communications and new distributed algorithms for distributed trust establishment.

In the security area, the researchers are developing algorithms that will detect self-propagating code. These algorithms will detect a change in the mean in distributed sensor systems and an exponential signal in noise or the mean.

They are also developing swarm intelligence-based trust evidence distribution. Swarm intelligence is biologically inspired by ants, bees, and other swarming creatures. Evidence requests are delivered by sending out multiple simple "ant" agents that travel the network and try to fetch information for the request. There is indirect communication between these agents and dynamic online optimization using local information. The advantages include simplicity, preserving the diversity of evidence, reinforcing good quality trust paths by feedback, discovering new sources of evidence via random exploration of the network and emergent behavior via continuous



Security. These charts depict a detection of self-propagating code simulation using sensor aggregation. In exponential waiting time, parametric statistics (Poisson arrivals) perform better. In Scale-free networks, detection delay depends on a few "key" sensors: the high degree nodes. In random networks there are no such "few high degree nodes," so they perform similar to random node aggregation.

work. The ants scheme can be used both for route and trust evidence discovery.

The MOCHA Project is developing middleware based on a code shipping architecture. Data sources are distributed and heterogeneous. Applications access and remote query is through economic deployment of the middleware and web-based GUI. The middleware keeps the data in place and moves the code instead, which is cost effective. The Java platform and XML standard makes this possible.

Support

Industry: APEX/ECLIPSE, Battelle, Boeing, Lockheed Martin, SAIC, Telcordia

Industry interest: Verizon, IBM

Other sponsors: Defense Advanced Research Projects Agency, Army Research Laboratory CTA C&N, Army Research Office, Maryland Industrial Partnerships, National Science Foundation, CECOM, University of New Mexico

Research Team

John Baras
Professor, Electrical and Computer Engineering and the Institute for Systems Research
Director, Center for Hybrid and Satellite Communication Networks

Virgil Gligor
Professor, Electrical and Computer Engineering

Michael Hadjitheodosiou
ISR Assistant Research Scientist

K.J. Ray Liu
Professor, Electrical and Computer Engineering and the Institute for Systems Research

Richard La
Assistant Professor, Electrical and Computer Engineering and the Institute for Systems Research

Nicholas Roussopoulos
Professor, Computer Science

ISR-affiliated faculty

Research staff: V. Bharadwaj and M. Karir

Graduate students: K. Manousakis, P. Dhasmaraju, H. Mehta, K. Chandrashekar, P. Ramachandran, A. Roy-Chowdhury, M. Striki, A. Cardenas, T. Jiang

Contacts

John S. Baras
Professor, Electrical and Computer Engineering Department and the Institute for Systems Research
2249 A.V. Williams Bldg.
University of Maryland
College Park, MD 20742

Phone: 301.405.6606
Email: baras@isr.umd.edu
Web: www.isr.umd.edu/~baras/

Link

Maryland Hybrid Networks Center
www.bynet.umd.edu