Logout
Home

Faculty Activity Reports

Bharat Bhargava

2005/06 Faculty Activity Report

Please return by Monday, March 13, 2006.

- Activities should cover the period March 2005 - February 2006.
- Publications should cover March 2004 - February 2006.

1. **Teaching** [Edit]

   Information about the courses you taught will be obtained from departmental records.
   To update teaching records please provide the following.

   1. List four to five CS courses you enjoy teaching. Please include at least two undergraduate courses.
      CS348, 448, 541, 542, 641, and 426
   2. Among CS 180, 182, 240, 250, and 251, list at least one course you feel comfortable teaching.
      Please note that listing none implies that you are comfortable teaching any of these courses.
      CS251
   3. Describe courses initiated or revised (major revision).
      CS542 (Distributed Database Systems) Updated this course with materials on privacy and security. Three new projects based on Pretty prototype have been initiated for students. Some new issues with wireless communications have been included.

      CS 690b: I am developing projects on Pervasive Systems. It included material on wireless, sensors, mobile adhoc networks, key management, and privacy. Potentailly this could be a new course for CS students in the future.
   4. Describe other teaching activities (e.g., summer conference courses, service learning, short courses).
      I video taped all my lectures for the distributed database course. They have been used by students in CS at Purdue and can be used for distant learning.
      I offered a small part of this material to students in Univ of Bern and National Technical University. This will be of help to future offerings for CS 542 students.
2. **Supervision of students** [Edit]

   1. Give the names of students who completed their PhD degrees under your supervision. Please indicate for each student (i) the level and type of support provided (RA, TA, fellowship) and (ii) his/her research area.
      Yuhui Zhong, Formalization of Dynamic Trust and Uncertain Evidence for User Authorization. RA, funded by NSF, 100%

      Weichao Wang, Security and Privacy in Pervasive Networks, RA, funded by NSF, 100%

2. Give the names of current PhD students supervised.
   Please indicate for each student (i) the level and type of support provided (RA, TA, fellowship) (ii) his/her research area, and (iii) whether pre-quals, post-quals, post-prelim, expected completion.
   Ding Gang, cross layer algorithms in wireless networks, RA, funded by NSF 100%, post-prelim (2006).

   Ahmet Can, Privacy in Databases, RA, funded by NSF 100%, post-prelim, (2006)

   Amit Shirsat, Topology control in wireless networks, post-prel, ITAP, (2006)

   Yu Zhang, RA funded by NSF 100%, post-qual I, 2008
3. PhD committee (post-candidacy) membership.
   This information is obtained from departmental and grad school records.
   Only provide corrections to the information you received.
   3
4. Individual graduate student projects supervised (including independent study courses).
   Please list student name, project title, and research area.
   Ahmet Burak Can, Privacy in Peer-to-Peer Systems

   Gang Ding, Cross-layer design and ZigBee Networks

   Faith Moulton, Energy Efficient Sensor Networks

   Wenchang Liu, Wireless Security and Privacy
5. Individual undergraduate student projects (including independent study courses) supervised.
   For each student, please list student name, project title, and research area.
   Gaurav Yadav, Wireless security (NSF-REU)
   Shawn Debnath, Pretty Systems development (NSF-REU)
   Roger Ellion, Network measurements (NSF-REU)
   Anurup Pavuluri, Alok Bhide, Jarav Desai, and Josh Olsen, Context aware mobile computing, CS 490 (coordinator Prof Aliaga)
6. Provide any additional information related to your interaction with students.
   Research Seminar on Distributed Systems & Networking, Spring 2005. Joint efforts with Prof. Fahmy, Yau, Xu, Park, Nita-Rotaru, and graduate students.

   Interact with students to participate in SoS undergraduate research day.

   Help minority students in retention in CS. Obtained REU grants to support two minority students from NSF.

   I encourage students to attend conferences. Students have attended ACM Multimedia Conference in Berkeley and PerCom conference, and sensor network conference.

   Meet visiting admitted graduate students. Available to students 24 hours via phone at home also.

   Invite students to home for informal discussions.

3. Research publications and presentations [Edit]

Please include the names of all authors in the order in which they appeared in the publication; also

include page numbers.
Publication should cover the time period March 2004 - February 2006.

1. Books, book chapters and book reviews.
   G. Ding, X. Wu, and B. Bhargava. Cross-Layer Algorithm for Video Transmission over Wireless Network, in Handbook of Algorithms for Mobile and Wireless Networking and Computing (A. Bourkerche, ed.), CRC Press, 2005.
2. Articles published in refereed journals. Distinguish between articles and correspondence items.
   PUBLISHED:

   M. Hefeeda, B. Bhargava, and D. Yau. A Cost-Effective Architecture for On-demand Media Streaming, Journal of Computer Networks, Vol. 44, Issue 4, pp. 353-382, March 2004.

   B. Bhargava, C. Shi, and S. Wang. MEPG Video Encryption Algorithms. Multimedia Tools and Applications, Vol 24, No. 3, 57-79, April, 2004.

   B. Bhargava, X. Wu, Y. Lu, and W. Wang. Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad Hoc Network (CAMA). ACM Special Issue of the Journal on Special Topics in Mobile Networking and Applications (MONET), (9), 393-408, 2004.

   B. Bhargava, L. Lilien, A. Rosenthal, and M. Winslett. Pervasive Trust, IEEE Intelligent Systems, Vol. 19, No. 5, 74-88, Sept./Oct. 2004.

   X. Wu, G.-H. Gary Chan, B. Mukherjee, and B. Bhargava. Mobile-Assisted Data Forwarding for Wireless Networks, in Journal of Communications and Networks, Vol. 6, No. 3, pp. 216-225, Sept. 2004.

   A. Habib, S. Fahmy, and B. Bhargava. Monitoring and Controlling QoS Network Domains, ACM/Wiley International Journal of Network Management, Vol. 15, Issue 1, Pages 11-29, Jan-Feb 2005.

   W. Wang, B. Bhargava, Y. Lu, and X. Wu. Defending Against Wormhole Attacks in Mobile Ad Hoc Networks, Wiley Journal on Wireless Communications and Mobile Computing, Vol 5, 1-21, 2005.

   B. Bhargava, S. Wang, M. Khan, and A. Habib. Multimedia Data Transmission and Contol Using Active Networks. Special Issue on Activated and Programmable Internet, Journal of Computer Communications Vol 28, Issue 6, Pages 623-639, April 2005.

   X. Wu and B. Bhargava. A02P: Ad Hoc On-Demand Position-Based Private Routing Protocol, IEEE Transactions on Mobile Computing Vol. 4, No. 4, 335-348, July, 2005.

   A. Habib, D. Xu, M. Atallah, B. Bhargava, J. Chuang. A tree-based Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming, IEEE Transactions on Knowledge and Data Engineering, 17(7), July, 2005.

   M. Hefeeda, A. Habib, D. Xu, B. Bhargava, and B. Botev. CollectCast: A Peer-to-Peer

Service for Media Streaming, ACM/Springer Multimedia Systems Journal, 11(1), Sept., 2005.

B. Bhargava, M. Jenamani, and Y. Zhong. Counteracting Shill Bidding in Online English Auction, International Journal of Cooperative Information Systems, 14(2-3), 245-263, Oct., 2005.

To Appear:

X. Wu, B. Mukherjee, and B. Bhargava. A Crossing-Tier Location Update/Paging Scheme in Hierarchical Cellular Networks. IEEE Transactions on Wireless Communications.

G. Ding, Z. Sahinoglu, B. Bhargava, P. Orlik, and J. Zhang, Tree-Based Data Broadcast in IEEE 802.15.4 and ZigBee Networks, IEEE Transactions on Mobile Computing.

G. Ding, X. Wu, and B. Bhargava, Performance Evaluation of Multiple-Rate Mobile Wireless Ad Hoc Networks, Performance Evaluation An International Journal.

L. Lilien and B. Bhargava, A Scheme for Privacy-preserving Data Dissemination, IEEE Transactions on Systems, Man and Cybernetics. (Based on best papers from Secure Knowledge Management conference)

Y. Lu, W. Wang, D. Xu, and B. Bhargava, Trust-Based Privacy Preservation for Peer-to-peer Data Sharing accepted to appear in IEEE Transactions on Systems, Man and Cybernetics (Part A), (Special Issue based on best papers from Secure Knowledge Management Conference).

M. Jenamani, Y. Zhong, and B. Bhargava, Cheating in online auction - Towards explaining the popularity of English auction, Elsevier Int. Journal of Electronics Commerce Research and Applications.

R. M. Garimella and B. Bhargava, Fundamental Limits on a Model of Privacy-Trust Tradeoff: Information Theoretic Approach, International Journal of Network Security.

Under Revision:

Y. Lu and B. Bhargava. SAGA: Self-Adjusting Congestion Avoidance Routing Protocol for Ad Hoc Networks. IEEE TMC

SUBMITTED:

S. Li, G. Chen, A. Cheung, B. Bhargava, On the design of perceptual MPEG-Video Encryption algorithms. (Under revision)

Y. Zhong, Y. Lu, B. Bhargava and L. Lilien, A computational dynamic trust model for user authorization.

Y. Zhong, Y. Lu, B. Bhargava and L. Lilien, An authorization framework based on uncertain evidence and dynamic trust.

X. Wu, G. Ding, and B. Bhargava, Impact of Link Distance on End-to-End Throughput in Multi-Rate Ad Hoc Networks.

A. B. Can and B. Bhargava, Anonymity for Trust Holders Using k-anonymity Chord.

A. B. Can and B. Bhargava, Selecting Trustworthy Service Peers based on Interaction Histories.

W.Wang, J.Kong, Z. Ji, R. Bagrodia, B. Bhargava, M. Gerla, Visulization of Wormholes in Underwater Sensor Networks.

3. Articles published in rigorously reviewed conferences with archival proceedings.

G. Ding and B. Bhargava. Peer-to-peer File-sharing over Mobile Ad hoc Networks, in Proceedings of International Workshop on Mobile Peer-to-Peer Computing, Joint with PerComm, Orlando, Florida, March 2004.

P. Ruth, D. Xu, B. Bhargava, and F. Regnier. E-notebook Middleware for Accountability and Reputation Based Trust in Distributed Data Sharing Communities , in Proceedings of 2nd International Conference on Trust Management (Springer Verlag), London, UK, March 2004.

M. Jenamani, L. Lilien, and B. Bhargava, Anonymizing Web Services Through a Club Mechanism with Economic Incentives, in Proceedings of International Conference on Web Services (ICWS 2004), San Diego, California, July 2004, pp. 792-795.

B. Bhargava and L. Lilien. Private and Trusted Collaborations, in Proceedings of NSF/NSA/AFRL Conference on Secure Knowledge Management (SKM), Amherst, N.Y., Sept. 2004. (Invited paper.)

Yi Lu, Weichao Wang, Dongyan Xu, and B. Bhargava, Trust-Based Privacy Preservation for Peer-to-peer Media Streaming, in Proceedings of NSF/NSA/AFRL Conference on Secure Knowledge Management (SKM), Amherst, NY, Sep. 2004. Selected as one of the two best papers)

Yuhui Zhong, and B. Bhargava, Using Entropy to Tradeoff Privacy and Trust, in Proceedings of NSF/NSA/AFRL Conference on Secure Knowledge Management (SKM), Amherst, NY, Sep. 2004.

W. Wang and B. Bhargava, Visualization of Wormholes in Sensor Networks, in Proceedings of ACM Workshop on Wireless Security (WiSe), in conjunction with MobiCom, October, 2004.

G. Ding, X. Wu, and B. Bhargava. A Simulation Study on Multi-Rate Mobile Ad Hoc Networks, in ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, Ubiquitous Networks, Venice, Italy, Oct. 2004.

B. Bhargava and L. Lilien. Vulnerabilities and Threats in Distributed Systems, in Proceedings of International Conference on Distributed Computing & Internet Technology (ICDCIT),Bhubaneswar, India, Dec. 2004. (Keynote paper.)

A. Habib, D. Xu, M. Atallah, B. Bhargava. "Verifying Data Integrity in Peer to Peer Video Streaming," in Proceedings of Multimedia SPIE/ACM Twelth Conference on Computing and Network (MMCN), Berkeley, January 2005.

G. Ding, Z. Sahinoglu, P. Orlik, J. Zhang, and B. Bhargava, Reliable Broadcast in ZigBee Networks, in IEEE Conference on Sensor and Ad Hoc Communications and Networks (SECON), Santa Clara, September, 2005.

A. Kumar, A. Bhargava, B. Bhargava, S. Madria, Adaptable Web Browsing of Images in Mobile Computing Environment: Experiments and Observations, in International Conference on Distributed Computing & Internet Technology (ICDCIT),Bhubaneswar, India, Dec. 2005.

R. M. Garimella, H. R. Gogineni, and B. Bhargava, Modeling Adaptive Routing in Wireless and Other Networks Using Coupled Queues, in the 12th IEEE International Conference on High Performance Computing: Workshop on Next Generation Wireless networks, Goa, December 18-21, 2005.

J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia, and B. Bhargava, Low-cost Attacks against Packet Delivery, Localization and Time Synchronization Services in Under-Water Sensor Networks, in Proceedings of ACM Workshop on Wireless Security (WiSe), in conjunction with MobiCom, 2005.

W. Wang, and B. Bhargava, Key Distribution and Update for Secure Inter-group Multicast Communication, in Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), in conjunction with ACM CCS, 2005.

B. Panja, S. Madria, and B. Bhargava, Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks, in IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC2006), June 2006. (To appear)

4. Other papers presented at conferences, symposia or workshops with published proceedings.
   Y. Zhong, Y. Lu, and B. Bhargava. TERA: An Authorization Framework Based on Uncertain Evidence and Dynamic Trust. Technical Report CSD-TR 04-009, Computer Sciences Department, Purdue University.

   B. Bhargava, C. Farkas, L. Lilien, and F. Makedon. Privacy and Security. Summary of a Workshop Breakout Session at the National Science Foundation Information and Data Management (IDM) Workshop held in Boston in Sept., 2004. CERIAS Technical Report 34, Center for Educational and Research Information Assurance and Security, Purdue University.
   https://www.cerias.purdue.edu/tools and resources/bibtex archive/archive/2003-34.pdf
   (Also on the web site of University of Washington set up for NSF.)

5. Publications in other media.
   S. Potluri, P. Venkatayogi, and B. Bhargava, Behavior-based System for Generation of Security Solutions, Technical Report, CSD TR 04-011, Department of Computer Sciences, Purdue University.

6. Invited presentations and keynote addresses at major conferences.

Keynote speaker during Research Day conference at Oakland University in Troy, Michigan, Oct., 2005

7. Presentations not listed above.
   W. Wang, and B. Bhargava, Location Privacy in Geographical Routing for Mobile Ad Hoc Networks, in Proceedings of NSF/NSA/AFRL Conference on Secure Knowledge Management (SKM), Amherst, NY, September, 2004.
8. Patents issued and software developed. Technology transfer efforts and industrial applications. Describe effort and impact.
   Ph.D student Gang Ding has applied for patents on his work on ZigBee networks based on his internship. This is joint work with Mitsubishi Corp and Intel. Extensions to Network Simulator (ns) with support for congestion avoidance routing protocol and intruder detection in mobile ad hoc networks. Additional extensions for privacy based on location, position, and time have been completed.

   Trust-enhanced role assignment (TERA) prototype decides whether or not a user is authorized for an access based on the policies, the evidence, and the trust value for a user. It consists of several trust enhanced role mapping (TERM) servers and a reputation server.

   A user application is provided to simulate different user behaviors for experimental studies. A user can connect to and interact with any TERM server. Her behaviors can be generated manually or according to predefine behavior models: stable, repenting, cheating, smart cheater.

   Using the TERA prototype, experiments are being conducted on evaluation of (a) behavior-based trust-building algorithms, (b) uncertain evidence handling mechanisms, and (c) personalized reputation calculation algorithms.
   The TERA prototype and its demonstration are available at http://www.cs.purdue.edu/homes/bb/NSFtrust.

   PRETTY
   Based on TERA, we are building a full scope prototype system called PRETTY (private and trusted system). PRETTY implements the research ideas in privacy-preserving data dissemination, quantification of the tradeoff between privacy and trust, and unified privacy metrics to provide quantitative assessment of the privacy level achieved by different techniques. PRETTY utilizes the server/client architecture. The client component of PRETTY consists of the user application, the credential manager, the evaluator of trust gain and privacy loss, the privacy negotiator, and a set of privacy policies. The server component consists of the server application, the TERA server, the privacy negotiator, the set of privacy policies, the database, and the data disseminator. PRETTY provides a platform to simulate privacy violators and users with different levels of trust. It will serve as a testbed for experimental studies on (a) clean self-destruction and proximity-based evaporation for private objects, (b) effectiveness and e1ciency of the probability-based and lattice-based privacy loss evaluation methods, and (c) evaluation of the dynamic mappings between trust levels and distortion levels.

   Cellular-Assisted Mobile Ad Hoc (CAMA)
   CAMA network is a integrated network for ad hoc networks to take advantage from the well-built cellular management system. Cellular network works as a centralized control to handle the ad hoc network management of routing and security in a position-based routing algorithm. Experiments are conducted on throughput, cellular signaling, and robustness to imprecise position information.

The simulator is built upon ns-2. In the link layer, the original program in ns-2 for CSMA/CA medium access mechanism is adopted in our simulations. In network layer, positioning routing program is developed. To test the performance when multiple rates are used for data transmission through wireless channel, we modified the judging packet receiving quality by using signal-noise-ratio (SNR) instead of power, since SNR determines transmission rate. Simulator is built to calculate the overall noise (including white noise and co-channel interference) to a receiver at the time a packet arrives. This is joint work with Motorola.

CollectCast: A Peer-to-Peer Service for Media Streaming (Joint work with Prof. D. Xu)
A new network service called CollectCast has been designed and implemented. CollectCast is targeted towards cooperative P2P media streaming applications that operate in a highly diverse and dynamic P2P networks. CollectCast is to be layered on top of a P2P lookup substrate and is comprised of four components: (1) topology inference and labeling, (2) peer selection, (3) rate and data assignment, and (4) monitoring and adaptation.

The topology inference component adapts network tomography techniques to infer the performance (e.g., segment-wise loss rate and available bandwidth) of the underlying network with low overhead. Network tomography means inferring the internal characteristics of a network by only probing it from the end points.
The adaptations we make on the basic inference techniques yield smaller convergence time and much less overhead, while maintaining the desired level of accuracy for the target P2P streaming applications. The peer selection component takes as inputs the set of candidate suppliers and the network performance information. It then uses this information in selecting the best senders for the streaming session.

Multiple concurrently sending peers are coordinated by the rate and data assignment component of CollectCast. The assignment technique allots each sender the appropriate rate and data based on the network performance information and sender's characteristics. To account for network dynamics and peer failures, the monitoring and adaptation component of CollectCast continually adjusts the sending rate of each sender, and switches failed senders by backup ones. Forward error correction (FEC) is used in an adaptive way to tolerate packet losses.

PROMISE: A Peer-to-Peer Media Streaming System. (Joint work with Prof. D. Xu)
PROMISE is a P2P media streaming system developed on top of CollectCast. The components of CollectCast have been implemented. We have developed PROMISE to assess the performance of CollectCast in real environments. PROMISE runs as an agent on each participating peer. In the implementation, we used Pastry as the P2P lookup substrate. Pastry returns a single supplying peer for each object lookup request, if the object exists in the system. We have modified Pastry to support multiple supplying peers for each lookup. These supplying peers form the candidate set for the peer selection algorithm.

PROMISE has been tested in both local and wide area environments. To test the code in the wide area environment, we have installed PROMISE agents on 15 nodes of the PlanetLab wide area test bed. The nodes chosen for the experiments are distributed over different geographic locations. Extensive experimental study on the performance of PROMISE has been conducted.

CollectCast and Promise System Software has been requested by fifteen universities.

These tools and software are used in CS 542, CS 641 and have been used by our funding agencies.

Our research on Cellular Assisted Mobile Ad Hoc Networks
(CAMA) is of great use at Motorola. We are now working with Jeff Bonta in Motorola to evaluate commercial value.

Efficient Multimedia Security Protocols.
This series of protocols combine the encryption and compression algorithms. Providing details and software to industry including Intel. (Twenty requests from various industry have been received.)

Working closely with IBM in applying adaptability software scheme to the Autonomic Computing program.

Working with Microsoft VP Javad Khaki for research collaboration in security and privacy. Trying to obtain support for Regenstrief Center for health care engineering.

Working with Google for further support for CS department.

ZigBee Networks
In a ZigBee network research project joint with Mitsubishi Corporation, we proposed two novel algorithms to find the minimum number of broadcast nodes to cover the whole sensor network, and to deal with the packet loss and inaccurate neighbor information. In this project, we have further collaboration with researchers in Intel and Motorola Labs.

Under-Water Sensor Networking (UWSN)
UWSN is a novel network paradigm that is being proposed to explore, monitor and protect the oceans. The unique characteristics of the aquatic environment, namely huge propagation delay, absence of GPS signaling, floating node mobility, and limited (acoustic) link capacity, are very different from those of ground sensor networks. Since underwater networks are mostly autonomous and very difficult to directly monitor by humans, a very important requirement is the built-in protection from automated malicious attacks. We show that the aquatic environment is particularly vulnerable to attacks and security must be integrated into the UWSN architecture to protect its localization, synchronization and packet delivery services.
This work has applications for Sunami type of disasters.

Privacy is needed in ad hoc networks.
An ad hoc on-demand position-based private routing algorithm, called AO2P, is proposed for communication anonymity. Only the position of the destination is exposed in the network for route discovery. To discover routes with the limited routing information, a receiver contention scheme is designed for determining the next hop. Pseudo identifiers are used for data packet delivery after a route is established. Real identities (IDs) for the source nodes, the destination nodes, and the forwarding nodes in the end-to-end connections are kept private. Anonymity for a destination relies on the difficulty of matching a geographic position to a real node ID. This can be enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary. To further improve destination privacy, R-2P is proposed. In this protocol, the position of a reference point, instead of the position of the destination, is

used for route discovery. Analytical models are developed for evaluating the delay in route discovery and the probability of route discovery failure. A simulator based on ns-2 is developed for evaluating network throughput. Analysis and simulation results show that, while AO2P preserves communication privacy in ad hoc networks, its routing performance is comparable with other position-based routing algorithms.
This work has applications for wireless service providers such as Cingular and Army.

4. Research [Edit]

1. Briefly discuss your research highlights for the last year.
   I am conducting research in privacy and security issues in mobile and ad hoc networks, privacy/trust issues in medical database systems, and vulnerability analysis and threat/risk assesment. Wireless security research involves host authentication and key management, secure routing, and dealing with malicious hosts, adaptability to attacks, and experimental studies. Database research involves formalizing evidence, trust, and fraud. Applications in e-commerce and medical data integration and dissemination are being tested in a prototype system. Schemes have been proposed to identify vulnerabilities in systems and networks, and assess threats to large organizations. I have developed techniques to avoid threats that can lead to operational failures. The research has direct impact on nuclear waste transport, bio-security, disaster management, and homeland security. These ideas and scientific principles are being applied to the building of peer-to-peer systems, cellular assisted mobile ad hoc networks, and to the monitoring of QoS-enabled network domains.

   The RAID laboratory at Purdue University has facilities to conduct both theoretical and experimental studies in networking. They include network communication measurement experiments, analysis of communication infrastructure, adaptability experiments for distributed systems, and peer-to-peer systems. Experimental studies involve a variety of subjects in security: secure routing and intruder identification in mobile ad hoc networks, authentication and key management in mobile systems, trust assessment and prediction, monitoring network domains to detect service violations and DoS attacks, and vulnerabilities and attacker behaviors.

   A major thurst of research has been in privacy schemes for networking (Internet as well as ad hoc) and peer-to-peer systems.
2. Information on current and pending research grants will be distributed by the business office.
   If any entries are not correct, please contact the business office.
   Below list awarded or pending funding activities not showing up on the business office report.
   This could include proposals not requiring a budget going through CS business office, gifts not yet recorded, or internal funding coming to the department on 10-funds.
   Please get information from Purdue Business Office.
3. List post-docs/research associates supported (and their current status).
   Dr. Leszek Lilien (2002-2005), funded by NSF. Joined Western Mich Univ.
   Dr. Xiaoxin Wu (2002)-2006), funded by NSF and I3P (Dartmouth). Will join Intel-China
   Dr. Rammurthy Gerimala (2005), funded by NSF. Is back to faculty position in IIIT India
   Prof. Jun Wen (2004-2005), visiting scholar. Is back to faculty position in China
4. Provide information on interdisciplinary research projects you are involved in.
   Please list project, nature of interaction, names of faculty in other departments, and any other relevant information. Indicate any Discovery Park activities.
   Joseph Pekny (Chemical Engineering) for Regenstrief Center for Health Care Engg
   Michael Zoltowski (Electrical and Computer Engineering) on ZigBee networks

Arif Ghafoor (Electrical and Computer Engineering) on Privacy research
Saurabh Bagchi, (Electrical and Computer Engineering) on NSF IGERT proposal
Bob McDonald at IU Medical School for Regenstrief Center for Health Care Engg.
Mario Gerla at UCLA (underwater sensors), Sanjay Madria at UMR (energy efficient data aggregation), Torsten Braun at Univ of Bern (networking and conferences)

Interaction involves writing proposals, research papers, and serving on PhD committees.

5. Service [Edit]

List committees you served on and events/activities you were actively involved in.
Include a brief statement as to your particular contribution.
For a list of committees see https://portals.cs.purdue.edu/home/dept/committee.shtml

1. Departmental committees.
   Informing members of the grad faculty about excellent students and helping the students in applying to Purdue. I believe my efforts have made a difference in the batch of students accepted by our department and I have helped in getting them to Purdue. I have been instrumental in coming with ideas to deal with Qual problems.

   Award committee: Evaluate undergraduate student applicants for annual awards,
   Support CS faculty for IEEE awards through committees

   Promotion Committee

   Internal Advisor Board of CERIAS: develop plans, guidelines for future research, teaching, and funding. Present results to visitors.

2. Departmental activities and events you participated in during the last year
   Multi-cultural Forum: Informed faculty of ideas to improve diversity.

   Presentation to admitted graduate students.

   Participate in Minority Award ceremony and represent department.

3. College of Science committees and events
   College of Science Research Committee.

   College of Science Committee for identification and recruitment of Minority Faculty.

   Member, College of Science Council and subcommittee on educational policy and curriculum.

   Food for tenure panel organized by Associate Dean.

   Health Database Planning Committee of Regenstrief Center for HealthCare Engineering

   Horizon Program: Mentor minority students, regular meetings with students and monthly meetings for one hour per month in different locations.

   Undergraduate Science Research Day Committee: I have coordinated the efforts in CS department on behalf of the School of Science.

4. University

   Active participant in CWSA and CERIAS.

   Member of team to write the successful proposal to establish Regenstrief Center for Health care Engineering.
5. Please indicate two categories which contain committees you are interested in serving in.
   Graduate (Study,Admission)
   Hiring (departmental, Coalesce, other)
6. Professional. Please include Journal editorial boards, conference program committees, and positions to advise and influence policy and priorities at the national level.
   * Editorial boards:

   Journal of System Integration.

   International Journal of Multi-Media Systems' Tools and Applications.

   International Journal of Cooperative Information Systems.

   IEEE Transactions on Mobile Computing.

   Wiley Journal on Wireless Communications and Mobile Computing.

   International Journal of Computers and Applications.

   International Journal on Systemics, Cybernetics, and Informatics

   * Committees:

   Steering committee of IEEE Symposium on Reliable Distributed Systems

   External Reviewer of Computer Science Department at Western Michigan Univeristy

   NSF PI workshop, Area Chair for Privacy & Trust Management.

   Panelist for IDM Career proposals, NSF, 2005.

   Panelist for Career proposals for SEII, NSF 2005.

   Panelist for Graduate Research Fellowships, NSF 2006

   IEEE Computer Society Fellow Committee, 2004-2006.

   * Technical Program Committees of Conferences:

   Chairman of Workshop on Distributed Systems and Networks in Bern, Switzerland, May, 2006

   Fourth International Conference on Wired/Wireless Internet Communications, Bern, May, 2006

IASTED International Conference on Wireless Sensor Networks (WSN), Banff, Canada, July 2006

First International Conference on Availability, Reliability, and Security (AReS),Vienna, April, 2006

International Conference on Information Security, Miami, Aug., 2006

IEEE International Symposium on network Computing and Applications (NCA-TNC), Cambridge, July 2006

IADIS Virtual Multi Conference on Computer Science and Information Systems (MCCSIS), May 2006

Security and Privacy in Communication Networks (SecureComm-06), Baltimore, Sept., 2006

Second International Conference on Web Information Systems and Technologies (WEBIST), Setubal, Portugal, April, 2006 (also member of first WEBIST conf in Miami, 2005)

IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks, Greece, Oct., 2005

ACM Workshop on Advances on Peer to Peer Multimedia Streams, Singapur, Nov, 2005

International Conference on Mobile Ad Hoc and Sensor Systems, Wash DC, 2005

International Conference on Wireless and Sensor Network Security, 2005

International Workshop on Research Challenges in Security and Privacy for Mobile Wireless Networks (WSPWN), Miami, March,2006

Technical Program Committee of Fourth International Conference on Mobile Business, Sydney, 2005.

Technical Program Committee of Fourth Annual Mediterranean Ad Hoc Networking Workshop, Porquerolles, France, 2005.

IEEE International Workshop on Web & Mobile Information System, Taiwan, March 2005.

IEEE International Workshop on Privacy Data Management, Tokyo, April 2005.

Fourth International Workshop on Assurance in Distributed Systems and Networks (ADSN) Columbus, July 2005.

Fourth International Conference on Mobile Business (m-business), Sydney, July 2005.

International Conference on Security and Privacy for Engineering Areas in Communication

Networks, August 2005.

International Workshop on Data Management in Global-Scale Data Repositories, Copenhagen, August 2005.

Second International Workshop P2P Data Management, Security and Trust (PDMST), Copenhagen, August 2005.

Program Committee of Workshop on Mobility in Databases & Distributed Systems (MDDS), Copenhagen, August 2005.

Security and Privacy in Communication Networks (SecureComm-2005), Greece, September 2005.

Seventh International Conference on Information Integration and Web-Based Applications and Services, Spain, September 2005.

International Workshop on Information Assurance in Distributed Systems (IADS), Nanjing, November 2005.

7. Mentoring of faculty and students (in addition to graduate students you are supervising).
   I read, revised and helped with the NSF Career proposal of Prof. D. Xu. I bring information about NSF, DoD opportunities to attention of junior faculty. Dong Yan and I went to ONR. I worked with Prof Zoltowski and his student Terry Charbonneau for a Darpa white paper. I got Prof. G. Pandurangan in an NSF proposal with Northwestern Univ.

   I have encouraged two minority graduate students who needed advice or were discouraged in CS courses. I tried to find research money for them. I am also helping minority students in other departments in finding research funds.
   I have spent a large amount of time in mentoring CS students in understanding our curriculum (qualifier exams, requirements) and encouraged them to stay for Ph.D. I am very active in recruiting efforts for new graduate students and in getting them internships at places where I have contacts. I was able to recruit Ashish Kundu from IBM (previously at IIT Bombay). I attended the National Communication Conference organized by all IITs in India and interacted with many students and encouraged them to apply to Purdue.

8. Provide any additional information relative to service that you feel is important.
   I believe I am providing leadership to the junior faculty. I nominated some of them to serve in the NSF panels and program committees of conferences. I have invited several faculty to the conference in Bern so that they can establish stronger ties with Switzerland researchers. I actively participate in undergraduate and award committees, faculty meeting, and CoS meetings.

6. Honors and awards [Edit]

List any honors/awards you received. Provide a brief description if appropriate.

1. University-wide activities
   Seed for Success Award for Regenstrief Center for Health Care Engg grant by Provost Sally Mason

2. Professional
3. Other

7. Other information [Edit]

1. Please describe activities related to diversity you have been involved in.
   I try to involve and support undergraduate minority students in Raidlab research projects. I obtained funding for three students from NSF-REU.

   I attended the Horizon program activities in addition to mentoring two students.

   I actively participated in identifying minority candidates and organized an informal visit by Prof. Janise McNair from Univ of Florida (colloquia).
   I identified several upcoming minority faculty candidates.

   I mentored and helped two graduate minority students and encouraged them for Ph.D.

   I attended the Multicultural Forum and informed faculty about the various aspects to increase interest.
2. Describe your most significant accomplishments and future plans in teaching, research and service this past year. Refer to above entries, if appropriate.
   Lack of trust, privacy, security, and reliability impedes information sharing, particularly among distributed entities. The potential for theft, fraud, harassment, and destruction of critical private data continues to exist. My research plan is to create knowledge and learning in secure networking, systems, and applications. Much of this research is based on using scientific principles for designing, building, evaluating systems in a living laboratory.

   There are fundamental research problems in privacy, trust, and security issues in collaborative systems. I briefly describe my planned objectives as follows:

   1 The first objective is to develop models of cyber attacks, identify vulnerabilities in systems and networks, and assess threats and losses. The risks associated with various types of attacks need to be studied. The timing, extent, scope, and duration of attacks will determine the adaptive strategy to deal with them. This research extends the best ideas from research in reliability and fault-tolerance. The research has direct impact on nuclear waste transport, bio-security, disaster management, and homeland security.

   2 The second objective is to investigate new ideas for privacy and security in networks. For mobile wireless networks research is needed in intruder identification under wormhole and coordinated attacks, and fault-tolerant authentication. For Internet the research questions deal with network monitoring and differentiated services for avoiding congestion and for the detection of service violations due to misbehaviors or attacks.

   3 The third objective is to formalize trust and fraud. Existence of system vulnerabilities provide opportunities for conducting fraud and create a threat to trusted collaborations. We plan to investigate fraud countermeasures and schemes for detection of swindler's fraudulent intentions. Fraudsters can be impersonators or swindlers. Experiments have been conducted to show effectiveness for various types of swindler's strategies. This research has applications to e-commerce and collaborations.

   4 The fourth objective is to research ideas that can help with integration and dissemination of private sensitive data. This includes measures of privacy and trust and tradeoffs between

the two. This research has applications to sharing of data among hospitals, government agencies, and commercial institutions. A series of experiments for adaptability, quality of service, P2P multimedia streaming, and privacy and trust tradeoffs will be carried out. Past research has resulted in several successful grants.

Research on vulnerability/threat assessment and security and privacy in databases have resulted in new measures, identification of tradeoffs, and practical schemes. Several prototype systems are under development to provide tools, measurements, and guidelines. All these ideas and scientific experiments contribute to the building of peer-to-peer systems, mobile ad hoc networks, and internet.

The details of ongoing research are available on my web site. I briefly present the current research activities.

A. Research in developing distributed monitoring schemes that use edge-to-edge measurements and collect statistics of delay, loss, and bandwidth in Internet has been published in collaboration with Prof. Fahmy. The objective is to reduce the overhead for core routers, deal with large scale network domains, and identify congested links to capture the misbehaving flows. Such flows violate service-level-agreements and inject excessive traffic that leads into denial of service attacks. The challenge is to investigate techniques to identify intruders and improve the performance for normal users.

A network service called CollectCast has been designed and implemented. CollectCast serves the applications that operate in diverse and dynamic networks. CollectCast can perform the topology inference, monitoring, and adaptation. The topology inference employs network tomography techniques to infer the performance (e.g., segment-wise loss rate and available bandwidth) of the underlying network with a low overhead. Network tomography infers the internal characteristics of a network by only probing it from the edge nodes. We are conducting similar research in wireless networks. Research involves the study of algorithm, protocol, and architecture design to improve quality of service (QoS) and security. Research topics include routing, security, and inter-networking in ad hoc/cellular integrated networks, multi-rate communication and real-time service over multi-hop wireless connections, and location privacy in ad hoc networks. For congestion measurements and avoidance in ad hoc networks, we have developed a SAGA protocol. SAGA uses intermediate delay (IMD) instead of hop count in routing decisions. The use of IMD enables selection of routes that bypass hot spots.

B. Research on intruder identification in ad hoc networks correctly identifies the malicious hosts in self organized infrastructures. This research is being done in the context of the AODV (Ad hoc On-demand Distance Vector) protocol. We are investigating coordinated attacks and wormhole attacks. Research involves host authentication and key management, secure routing and dealing with malicious hosts, adaptability to coordinated attacks, and experimental studies. Cellular-Assisted Mobile Ad hoc (CAMA) is network software for ad hoc mobile nodes that takes advantage of a cellular system. Cellular network works as a centralized control in a position-based routing algorithm to handle the ad hoc network management of routing and security. Experiments are conducted on throughput, cellular signaling, and robustness to imprecise position information. We are conducting experiments on the use of visualization of wormholes in underwater sensor networks.

C. Research in privacy and trust involves activities that range from simple transaction based interactions to the most complex collaborations. This involves algorithms to evaluate privacy loss and trust gain, mechanisms for disseminating data without compromising privacy, and assessment metrics that measure the privacy. Guidelines are being developed for a variety of applications for developing privacy policies, building trust, and determining strategies for disseminating data to trusted or unknown users. Applications in e-commerce and transportation security are being tested in a prototype system. An authorization for an access is based on the policies, the evidence, and the trust value assigned to a user. The reliability of evidence is determined by the trust value of the evidence provider and her own confidence level with respect to her opinions about the evidence. A user interacts with a role-based access control (RBAC) enhanced application server to provide role assignment information and obtain data on users' behaviors. Users' trust information is submitted to the reputation server. When the server encounters a new user or an old user in a new context, it requests the reputation server to compute the personalized reputation of the user by using the specified reputation evaluation algorithm. If there were any previous interactions with the user, a valid reputation value will be returned. This value is used as the trust value for role assignment and access. Using the TERA prototype (details on my web site), experiments study the evaluation of (a) behavior-based trust-building algorithms, (b) uncertain evidence handling mechanisms, and (c) personalized reputation calculation algorithms.

D. Research has been published in peer to peer multimedia streaming and video-on-demand applications. The system organizes peers in network-aware clusters that can allow for fast dissemination of multimedia files and control of traffic on the underlying network. File contents are distributed over the Internet in a cost-effective manner while achieving the desired quality of service. Further study includes economic models, privacy issues, verification of integrity of packets received by a peer, and privacy preservations. The description of various systems and prototypes are available in the activity report on my web site.

E. Efficient and Reliable Communication in ZigBee Networks. The ZigBee network is a low data rate, low cost, and low power ad hoc network based on IEEE 802.15.4 standard. It finds its use in industrial control, monitoring, and sensor networks. The ZigBee standards were approved at the end of 2004. Research activities have been persued to evaluate the feasibility and improve the performance of ZigBee networks. In contrast to other ad hoc networks, the ZigBee network is characterized as limited bandwidth, low power, and low computation capability. It is critical to find light-weight algorithms that use small amount of computation and communication resources to facilitate efficient and reliable communications in ZigBee networks. Contributions include: a) Development of polynomial time algorithms for minimizing the number of broadcast nodes while covering the whole network. For ad hoc networks this problem is NP-complete but for Zigbee networks we achieve this by taking advantage of network address assignments. b) Reliable algorithms to deal with in accuracy of neighboring nodes table or packet loss by adjusting the optimal solution and increasing the redundancy of communications. c)Increase security of multi-hop communication in Zigbee network and maintain trust in distributed nodes. d) Build an open source test-bed for experiments that will lead to successful transfer of implementations in industry. Experiments will evaluate the performance of efficiency and reliability of proposed algorithms and provide insights in their use in sensor networks

F. A Decentralized Trusted System for Preservation and Authentication of Online Multimedia Documents.
This project will address key problems attendant on the unprecedented accessibility of online multimedia digital documents. The problems stem from the vulnerability of the

documents to corruption and tampering in an open, peer-to-peer, and possibly malicious environment. Preservation of content, format, presentation, and functionality of stored documents is imperative in designing, managing, and governing reliable infrastructures for multimedia information in digital libraries and online documents. The research aims to provide solutions to preserving and authenticating large digital multimedia documents that are sharable in a decentralized environment. The solutions will be packaged as a toolbox called RAMPART (Robust Archiving of Multimedia-documents using Perceptually-based Authentication & Recovery Techniques), which also means protection, defense, or bulwark. The leading current approach on keeping documents relies on maintaining a large number of copies and using mechanisms to collect, store, preserve, and provide access to local copies of authorized documents. Key challenges pertaining to multimedia documents are: a) Multimedia documents, such as video archives, can be very large. Keeping a large number of copies? of very large files may not be feasible, b) Preservation and recovery using a collaborative approach is fraught with complexity issues in comparing large files, c) Trustworthiness of sites where the copies are stored may be variable. Trust management should be factored into the recovery of tampered multimedia content using a collaborative approach. In addition, multimedia documents offer opportunities for safekeeping that can be exploited in preservation and recovery: (i) Media attributes of amenability to imperceptible insertion of data and document signatures can offer feature-rich alternatives in document comparison and preservation. (ii) Data hiding offers mechanisms for running self-checks using secret keys within media objects comprising a document and across objects. (iii) Apart from content, multimedia documents have author-specified spatio-temporal, logical, and functional structures for organizing and orchestrating objects that may include audio, image, text and video data. Data embedding affords a preservation technology that captures such structure in documents and guarantees its preservation. (iv) Dynamic multimedia documents with shared objects further exacerbate the challenges in data hiding based authentication/recovery solutions and enhance opportunities for innovative applications of data hiding techniques. The research is based on unique application of data hiding technology and robust distributed multiparty encryption and trust mechanisms requiring collaboration of researchers and synthesis of ideas from different disciplines such as multimedia security, signal processing, databases and distributed systems. It will investigate: (i) New hierarchical signature models for hiding data in multimedia documents that will enable efficient collaborative authentication and preservation. (ii) Robust techniques for imperceptibly hiding data with suitable redundancy will be investigated for embedding hierarchical signatures framework within a multimedia document such that the embedding is robust to tampering of content and supports distributed authentication and recovery in a decentralized environment. (iii) Methods will be investigated for capturing and hiding spatio-temporal, logical, and functional relationships within individual media objects bit streams and across multiple media objects constituting a document. (iv) Efficient protocols for preserving, locating, authenticating, and recovering multimedia documents based on novel trust mechanisms in a decentralized P2P environment will be designed. The proposed research will provide a deeper understanding of the problems in multimedia document preservation and authentication and it will facilitate the development of innovative techniques for annotation formats and summarizing content in multimedia documents. The proposed effort is intellectually unique in the following aspects: A new approach to preservation and authentication of documents is required due to the constraint imposed by file size, structure and sharing characteristics of objects, and by the opportunity to exploit the inherent attributes of the media for hiding data. Novel hierarchical signatures will be developed for use in practical low-complexity algorithms for effectively performing document preservation and authentication in a P2P environment. This research is a joint efort with faculty in Univ of Ill-Chicago.

G. Power-efficient Sensor Network for Secure Routing and Aggregation
against Possible Attacks.
Wireless sensor networks are envisioned to consist of large numbers of motes, each capable of operating in an unattended mode with limited energy, computation and communication capability. Applications for detecting malfunctions, failures, and natural disasters require constant real-time monitoring against malicious and hostile activities. Since communication over the radio is un-secure and energy-consuming, it needs to be optimized. The challenge is to detect and determine events that interfere with safe operations of critical infrastructure monitoring such as observing water resources or patient monitoring in the health care industry. We plan to design the sensor network architecture for secure routing and aggregation to protect against attacks. The attacker can tamper with the data message, or selectively forward data messages. Solutions have been proposed to defend the sensor networks against the wormhole attack during the neighbor discovery process with the usage of some special hardware such as the directional antenna or the precise synchronized clock. The focus is on detecting such malicious nodes. We propose to build a secure route against such attacks with the objective of continuously tracing a secure path avoiding nodes compromised by black and worm holes without using any special hardware, clocks, or GPS devices. The objective of the protocol is to guarantee that the data reaches the sink node even if black or worm holes exist in the path. In secure aggregation, the sensor nodes at the lower-level sensor nodes only sense and disseminate data, whereas the higher-level sensors do secure aggregation and find the secure path to the sink node. We plan to work on an approach that uses watermarking for both security as well as verification. The main idea lies in the manner in which multiple watermark embedding locations are calculated. Each sensor value is broken into several segments. The least significant segment remains unchanged and is used along with a secret key to determine an embedding location in the most significant segment. That segment is then used to calculate the embedding details for the next significant segment and so forth. This allows for a significant change of the value that is being routed and hence provides needed security. Only bits of the value are flipped, so the payload size does not increase and no additional energy is needed to transmit the packet. This approach focuses on secure information processing in wireless sensor networks to better protect data against eavesdropping, spoofing and injecting of messages to ensure that the base station receives the intended data and can trust the received readings. This research activity will result in: a) New energy-efficient algorithms for secure routing against attacks and secure aggregation, b) Understanding of the fundamental problems and solutions of secure sensor routing and data aggregation, c) Design of innovative energy-efficient watermarking techniques for both data security as well as verification, d) Experimental evaluation of the proposed schemes that would determine the performance parameters for secure routing under various types of attacks, e) Sensor test-bed integration with the proposed research that will be made available for teaching and training. This research effort is joint with Univ of Missouri-Rolla.

H. Dynamically Adjustable Routing with Energy and Context Awareness in Sensor Networks. Recent technological advances have resulted in a development of small and relatively inexpensive sensors that are capable of monitoring and measuring various values of the physical world: temperature, humidity, pressure, acoustics, and many other chemical, mechanical and electromagnetic phenomena. Each sensor node is equipped with a memory and limited computational capabilities and, most importantly, a communication module which enables a set of deployed sensors to independently organize themselves into a wireless sensor network. These networks of cooperating
nodes engaged in various real-time tasks have spurred novel application domains, many of

which are processing requests that are data-centric in nature, such as continuous queries and detection of various events, which span over large geographic areas. A sensor network that is context aware needs to take into account the semantics of each individual request, types of the nodes involved, security requirements, as well as other quality constraints. To better organize the joint processing and timely dissemination of the data items of interest, the network needs the ability to adjust its topology and routing structures in a manner that will balance the quality expectations and the energy expenditures. The research will provide dynamically adjustable routing structures that will ensure the desired levels of security and quality for the data, while optimizing the energy expenditures and network's lifetime. We consider the evolution of the network in a context-aware manner, both with respect to the semantics and the dynamics of the arrival of the pending requests, as well as with respect to cooperation among the (networks of possibly heterogenous) nodes. Furthermore, we will investigate the efficient maintenance and retrieval of the overall concept of a state of the network, at different levels of granularity and semantics desired, e.g., for sub-regions, for types of requests and for monitoring the quality of service assurances. A noteworthy observation, as we will demonstrate in the proposal, is that attempting to minimize the total energy expenditure of a single routing structure corresponding to a particular continuous request (query and/or notification) in isolation, need not imply that the service-lifetime of the network as a whole is prolonged. Thus, an important aspect of our work will be ensuring the balance between the local, per-node and per-request energy efficiency, with the overall lifetime of the network. We will develop test-beds that will enable experimental validation of the benefits of our methodologies. This research is joint with faculty at Northwestern University and Prof. P. Pandurangan.
OVERVIEW:

My research plan is based on current grants, ongoing student thesis, and submitted proposals. Collaboration with faculty (Prof. Pandurangan and Prof. Xu) in Computer Science department, ECE, CWSA, and CERIAS can lead to proposals to DoD and NSF. One of my major objectives is to write proposals for centers.

In research, our group has developed several new ideas in mobile wireless networks, vulnerabilities, intrusion detection, QoS and DiffServ, intruder identification, fault-tolerant authentication, and detecting service violations in the Internet and mobile ad hoc networks. Trust and Fraud have been formalized. A series of experiments for adaptability for quality of service, P2P systems, multimedia, mobile ad hoc networks, and trust management have been carried out. My research resulted in several successful new proposals and three PhD thesis.

My work on vulnerability/threat assessment, security and communications in data warehousing, adaptable video conferencing, and mobile databases has created new directions of research.

Ideas of diffserve and adaptability have generated funds from SwissNSF and NSF. Adaptability mechanisms will be investigated for dealing with failures, providing different quality of service to different users, and providing different routing facilities to different packets. All this work is experimental and a lot of software infrastructure is being produced that will help in CS 542, CS 448, CS 348, and CS 641.

I participate actively in diversity activities, undergrad research day, grad committee, and help every minority students. I am passionate about helping underserved students.

I am active in recruiting new graduate students. For example, I worked hard to get Ashish Kundu.

Graduate two PhD students.

I am recruiting two more Ph.D. students and would like to work on graduate committee to update the curriculum. With Walid Aref and networking group, I like to set up a laboratory for Multimedia Systems courses. I worked on a University Research Fellowship from Motorola for Gang Ding and IBM fellowship for Weichao Wang.

Generate research in pervasive systems that can lead to a new graduate course.

In research, I like to collaborate with several systems faculty and build on top of my collaboration efforts of last year.
I would also like to provide the Raid laboratory facilities (software, experimental infrastructure, tools) to students of other faculty to create a good environment for experimental computer science. The direction of my research efforts in adaptable quality of service, network measurements, multi-media communication, active networks and digital library are on my web page www.cs.purdue.edu/homes/bb.

I have worked on an ONR proposal on cellular/mobile networks.

Collaborate and write proposals with Mike Zoltowski in ECE.

I like to bring more IEEE workshops and conferences at Purdue as part of my service activities. My major effort will be in getting industry funding for research and building the momentum for centers in CS dept. I like to help with raising funds for the department. I have contacted a few people at CISCO and a security company (owned by my roommate from Purdue) in Washington DC and Google where one of my student is an executive.

3. In your opinion, what are the most significant challenges and problems facing the department?
Improve Ranking. Involve faculty in new intitiatives and research teams.

Retain and help minorities and underserved students.

Retain CS students and increase enrollments.

Improve graduate curriculum, improve core courses, and revitalize qualifier examination.

Get a large interdisciplinary grant with SoS faculty/CERIAS.

Identify and reward the best faculty and students.

Retain/recruit the best faculty.