REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE 20 June 2006	3. REPORT TYPE AND DATES COVERED Final Report; 20010501-20060430

4. TITLE AND SUBTITLE
Modeling and Simulation Environment For Critical Infrastructure Protection

5. FUNDING NUMBERS
DAAD19-01-1-0502

6. AUTHOR(S)
Stephen M. Robinson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Board of Regents of the University of Wisconsin System
c/o Center for Human Performance and Risk Analysis
University of Wisconsin-Madison
1513 University Ave, Madison, WI 53706-1572

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
42347.38-MA-CIP

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This project integrated diverse disciplines to provide multidisciplinary analysis, understanding, and remediation of problems in the protection of critical national infrastructures. The project included basic mathematical and engineering analysis of structure and properties, analysis of human factors aspects both of the system operations and of the acts of intelligent adversaries including red teams, and computer-science approaches to problems such as automating detection of intrusions and responses to restore effectiveness after attacks.

The project goals were: (1) Develop models, software,and simulation tools for detection, characterization, and assessment of vulnerabilities in networked, interacting systems; (2) Develop understanding of the underlying phenomena and technological opportunities in systems employing hybrid human, physical and informational architectures, and build models and simulation environments suited to such systems; (3) Identify key vulnerabilities and develop principles for reducing vulnerability to human intrusion in networked systems; (4) Explore the use of models and simulation, together with evolving knowledge in human factors engineering; (5) Synthesize ideas and techniques across several tasks towards conducting pilot studies to establish proof of principle.

The project work consisted of activities in the following broad sub-areas: (1) Identification, detection, and characterization of vulnerabilities, (2)Resilient system architectures, (3) Integration, synthesis, and impact.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Critical infrastructure, networked system, intrusion detection, resiliency, reliability, human factors	40
	16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev.2-89)
Prescribed by ANSI Std. 239-18
298-102

Modeling and Simulation Environment For Critical Infrastructure Protection

FINAL REPORT

20 June 2006

Grant DAAD19-01-1-0502
1 May 2001 – 30 Apr 2006

Statement of the problem studied

This project integrated diverse disciplines to provide multidisciplinary analysis, understanding, and remediation of problems in the protection of critical national infrastructures. The project included basic mathematical and engineering analysis of structure and properties, analysis of human factors aspects both of the system operations and of the acts of intelligent adversaries including red teams, and computer-science approaches to problems such as automating detection of intrusions and responses to restore effectiveness after attacks.

The project *goals* were stated as follows in the original proposal:

- Develop models, software, and simulation tools for detection, characterization, and assessment of vulnerabilities in networked, interacting systems. These models will emphasize integrity and availability, and will facilitate development of methodologies for mitigating potential vulnerabilities in such systems and for restoring operation of failed systems.
- Develop understanding of the underlying phenomena and technological opportunities in systems employing hybrid human, physical and informational architectures, and build models and simulation environments suited to such systems.
- Identify key vulnerabilities and develop principles for reducing vulnerability to human intrusion in networked systems.
- Explore the use of models and simulation, together with evolving knowledge in human factors engineering, to replace conventional red teaming in exploring vulnerabilities of infrastructure systems.
- Synthesize ideas and techniques across several tasks towards conducting pilot studies to establish proof of principle.

The project *work* consisted of activities in the following broad sub-areas:

- *Identification, detection and characterization of vulnerabilities.* Here we concentrated on the development of a rigorous framework for identification and characterization of threat scenarios, and classification and measures of vulnerability. Such a mathematical framework lends itself to the development of reliable tools for performance assessments of complex interactive and interdependent critical infrastructures. Our objectives were to develop robust models and procedures for fusing information from multiple sources, data mining and case based reasoning for determining anomalous user behavior as well as patterns of intrusion and failure, and evaluation of software vulnerabilities.
- *Resilient system architectures.* Here we worked to develop a system architecture for automatically detecting and responding to potential threats and vulnerabilities in critical infrastructure systems. The key idea of such architectures is to maintain the original structure of the system with automatic reconfiguration of the system when a certain number of nodes fail.
- *Integration, synthesis and impact.* Deriving maximum benefit from the research efforts described in the preceding two sections required a concerted effort for the integration of ideas, tools and techniques. To this end, we established two test bed efforts for integrating and exercising methods developed in this effort.

Summary of the most important results

Identification, detection and characterization of vulnerabilities

Applications of filtering methods to computer security

Thomas Kurtz and associates explored application of filtering methods to computer security, in joint work with Somesh Jha, UW-Madison Department of Computer Sciences. The models developed assume that commands from a malicious user or intruder are interspersed in a stream of ordinary traffic, which itself may be the merger of streams from several different sources. The models are formulated in such a way that the commands from the intruder can be viewed as a "signal" contained in "noise" (the ordinary traffic). This formulation allows one to apply methods of optimal filtering to derive recursive algorithms that estimate the rate (and perhaps also the type) of intrusive activity.

The simplest of these models is for anomaly detection in input streams from a single user. Preliminary results were presented by Yoonjung Lee at the Filtering 2002 Conference in July 2002 in Edmonton, Canada. A complete presentation of these results is still in preparation.

A second problem is concerned with masquerade detection. In this situation an intruder or other user attempts to make illegitimate use of a system by posing as a legitimate user. Our model assumes that commands from the intruder are interspersed in a stream of ordinary traffic. The commands from the intruder form the "signal" in the filtering problem while the ordinary traffic is the "noise." The filtering methods are similar in spirit to Bayesian approaches taken by other researchers; however, these earlier methods assume that the observed commands come in large blocks from individual users and the method attempts to identify which blocks corresponds to which users and whether any of the users is illegitimate. The filtering method attempts to estimate the level of activity of individual users and to determine the presence of an illegitimate user (with a nonzero activity level).

A third model was motivated by the problem of detecting stealthy port scans, but may be of greater interest in other areas. The basic model is similar to the model for masquerade detection; however, the model for the "signal" is significantly more complex, and the dimensionality of the computational problems presents a major challenge. Zhengxiao Wu has introduced a simplified model for the signal which leads to a computationally feasible algorithm. The algorithm has been successfully applied to the identification of earthquake aftershocks. Work in this area will form the core of Wu's PhD dissertation.

Statistical methods for spatial and other marked point processes

Markov chain Monte Carlo has become the standard approach to simulation of stochastic models for spatial point processes. Central to this approach is the assumption that the model gives the stationary distribution of a Markov spatial birth and death process.

Traditionally, one characterizes the model first and then finds the Markov process that has the given model as its stationary distribution. Joint work of Thomas Kurtz with Shun-Hwa Li characterizes the model directly by specifying the birth and death process first and then taking the corresponding stationary distribution to be the desired model. The time-invariance estimation methods introduced by Adrian Baddeley then provide a natural approach to estimating the parameters of the models.

The analysis of these parameter estimates leads to fundamental theoretical questions on the properties of spatial birth and death processes that were studied in collaboration with Nancy L. Garcia of Universidade Estadual de Campinas, Brazil. Theoretical work in this area is focused on the development of effective representations of stochastic models as solutions of stochastic equations driven by Poisson random measures. These representations are highly flexible modeling tools, and also enable one to employ a variety of stochastic analytic methods in the analysis of the resulting models.

Authentication and verification of security protocols

The authentication and verification of security protocols are complex analytical procedures with the overhead of expert human interaction. The vulnerability and importance of computers, robots, Internet etc, demand the employment of exceedingly reliable security protocols. The extraordinary human analytical abilities required in the verification procedure result in the presence of security leakages in a protocol. The group led by Ratan Guha at UCF designed a heuristic state space search model for automatic security protocol verification. The attributes of security protocol are represented formally and verified using logic of authentication. An efficient algorithm is used for the verification procedure. The simplicity of our approach enables it to be translated into existing solutions for greater efficiency. The aim is to minimize the flaws in simulation and increase the efficiency of protocol verification procedure.

Strand Space Method (SSM) is a widely appreciated method for security protocols analyses. It models a Dolev-Yao intruder in terms of strands of various kinds and analyzes a protocol by applying all combinations of intruder strands in search for a successful attack. We highlight the usefulness of a common challenge-response criterion for analyzing authentication protocols. For this purpose, we use strand space formalism to develop principles that guarantee if a participant has successfully answered the authentication challenge in a protocol. Correct answer to a participant's challenge implies that the intended participant has actually received the challenge, thereby agreeing to a set of parameters between both participants. The proposed principles are a result of applying several attack strategies by a potential SSM intruder. We posit that a protocol satisfying these principles is tantamount as if it has been analyzed for different attack strategies by an active Dolev-Yao intruder. We construct a formal framework that realizes the proposed principles in terms of rules in many-sorted modal logic. We lay out a computational model and provide semantics of logical constructs in that model. We apply our approach on a wide variety of security protocols to demonstrate how we can benefit from the expressiveness of strand space machinery and the simplicity of logic based approaches.

While benefiting from the express ability of strand diagrams, we devised a set of rules using strand space formalism for analyzing authentication protocols. We also highlight the usefulness of a common challenge-response criterion for this purpose. A protocol is analyzed by finding out the challenge generated by a participant of the protocol and then by applying the set of proposed rules in order to find out if the intended responder(s) have successfully answered the challenge. A correct answer to a participant's challenge implies that the intended participant has actually received the challenge, thereby agreeing to a set of parameters between the participants. The need for providing assurance in parameter matching in authentication protocols is emphasized by analyzing a variety of well-known protocols. Authentication protocols achieve their goals when a participant guarantees its set of parameters to be in accordance with that of the rest of the participants of the protocol. On the other hand, the lack of guarantee suggests possible venues for attacks by a saboteur. Some of the example protocols exhibit this lack of assurance in parameter matching among participants and hence succumbed to subtle attacks presented in this paper.

Intrusion prevention

To date, worms and other network-based attacks have gained unauthorized access to hosts by exploiting *known* software vulnerabilities that can be exploited through the network. The group led by Mary K. Vernon at UW-Madison studied the problem of intrusion *prevention* by extending the state of the art in tools that audit a system of networked hosts to identify and repair such software vulnerabilities. Broad goals of this research included (1) delineating the scope of the vulnerabilities that can be audited by such tools, (2) improving the scope as well as the accuracy of the vulnerabilities that are identified, and (3) providing a new and significantly more powerful threat analysis of the vulnerabilities that are uncovered. In one of eight papers selected at the “best and most interesting papers at DIMVA 2004”, we (1) provide new foundations for intrusion prevention in the form of a proposed infrastructure for identifying, evaluating and repairing vulnerabilities to prevent intrusions, and (2) apply the new foundations in a large scale experiment. The new foundations include a proposed vulnerability semantics – a small set of attributes and predicates that can be used to define known vulnerabilities in a way that facilitates their accurate identification. The new foundations also include a more powerful site-customizable threat analyzer that ranks each uncovered vulnerability according to the attack severity, the site-specific attack difficulty, and the site security policies. The experiment demonstrated the identification and repair of significant, previously undetected, long-lived vulnerabilities in a system with over 1500 hosts and a high security awareness.

As part of the research published in DIMVA 2004, we developed a significantly enhanced Threat Analyzer for the Nessus audit tool, and we created a semi-automated process for running the audit and threat analyzer on large systems. The extended tool automates an efficient and low-impact networked systems audit, and stores the results in a database for querying and for tracking changes in the system audits. This tool was used on a bi-weekly basis to audit the 1500-host networked system of the Computer Systems Laboratory (CSL) of the Computer Science Dept. at the University of Wisconsin-

Madison. This networked system contains over 75 critical servers, running Windows, Linux, Solaris, FreeBSD, and Tru64. The biweekly audits uncovered significant vulnerabilities previously unknown to the system administrators. The new tool was also distributed to the State of Wisconsin Department of Health and Family Services (DHFS) for use in complying with recent new regulations for insuring greater security for networked information systems owned by the State. Informal feedback provided by DHFS indicated that the tool was significantly improving the security of their systems. Notably, it has pinpointed vulnerable software that they were not aware was running on their key systems, which facilitated removing the vulnerabilities.

Protecting sensor host anonymity

Maintaining the anonymity of the hosts in widely distributed sensor networks that sense malicious traffic on the Internet is critical so that malicious attackers won't be able to bypass the sensors when carrying out their attacks. The research on protecting sensor network anonymity included two broad questions. First, is it possible to quickly discover the identity of the sensing hosts in networks that use current methods for protecting host identities? Second, what improvements can be made in protecting host identity?

In a 2005 USENIX Security Symposium paper that won the Best Paper Award for the conference, we develop a divide-and-conquer probing method that can determine the IP addresses of the sensing hosts in Internet sensor networks that monitor malicious activity on the Internet. The most significant result in the paper is that using the attack statistics that are commonly published, the new probe method can fully map the locations of the sensors in a network that contains many thousands of widely distributed sensors in a small number (e.g., 0.5-4) days if the probing host has a sufficiently high bandwidth connection to the internet (e.g., a T3 connection). The paper also enumerates various countermeasures that sensor networks might employ to make the probe method infeasible, including randomly discarding a very small fraction of the sensor activity that is reported. This work was the first research paper experience for undergraduates John Bethencourt and Jason Franklin, both of whom are now actively publishing graduate students at Carnegie-Mellon University.

Case-based approach to multi-sensor network intrusion detection

The team at Florida State University, Department of Computer Science, has investigated the general problem of multi-sensor computer network intrusion detection. Sensors may be stand-alone intrusion detection systems (IDSs) of various types. These can be classed as misuse detection, looking for signatures of previously experienced attacks, or anomaly detection, looking for new kinds of attacks as deviations from expected normal system behavior. Such sensors include network-based IDSs that monitor traffic in and our of a network, host-based IDSs that monitor system calls on a particular node (host computer) in a network, as well as firewalls, antivirus software, and any other intrusion detection mechanism that can fire alerts.

A critical issue in multi-sensor intrusion detection is *alert correlation*; that is, determining which alerts coming from the various sensors are associated with the same attack. This becomes especially challenging when the network is subjected to several

simultaneous attacks. Thus a substantial portion of our effort has focused on this particular problem.

The early part of our work entailed development of an Adaptive Case-Based Reasoning Software Framework. This is a software package that enables one to rapidly create a case-based reasoning (CBR) system for any of a wide variety of different types of application domains. It also enables one to easily modify a particular CBR system, or experiment with different kinds of cases, for a given application domain. The framework and its use are briefly as follows.

A *case* is a *problem-solution* pair, where a problem is described by a set of *features*. Cases are represented in XML, with the structure of the cases (the problem features and solution) for a particular application domain being defined by an XML schema. A library of such cases is created, where each case represents a previously experienced event. The XML schema can be fed into Sun Microsystems JAXB (Java for XML Binding) to produce all the Java classes necessary for parsing XML documents that adhere to that schema. These classes are then imported into a search engine framework, in effect, instantiating the framework, to create an engine for searching the given case library. The search engine can take as input any problem, represented in XML according to the schema, and return all cases in the library whose problem parts are *similar* the that problem.

Implementation of the *similarity measure* used for this purpose employs a modern software methodology known variously as “adaptive”, or “reflective”, or “metadata” architecture. This has the effect of separating the domain independent aspects of the search engine from those that are domain dependent. For each problem feature there is an associated *comparator*, which measures the similarity between that feature’s occurrence in the input problem and that same feature’s occurrence in a case in the library. Comparators return values between 0 and 1, representing the degree of similarity for that feature. The results of the comparators for all the features in a problem are then combined, using some *feature combination rule*, to produce a final value between 0 and 1, representing the overall similarity between the given input problem and the case.

Several different features may use the same comparators, the same comparators may in fact be reused across various application domains, and new comparators may need to be created for new features not previously encountered. Which comparators are to be used for which features in a given application is recorded in a file as metadata. Then, during run time, when searching for cases that are similar to an input problem, this *metadata* file is consulted for each problem feature to determine which comparator is required, the corresponding comparator is instantiated dynamically using the Java methods for class *reflection*, and the comparator is then applied. This architecture is *adaptive* in that the framework can be adapted to new kinds of cases, with new feature sets, simply by changing the entries in the metadata file and, possibly, writing new comparators as needed for any new kinds of features.

Given this CBR framework, the effort then turned to the problem of multi-sensor network intrusion detection, which we came to term *meta-intrusion detection*. Three experiments were conducted. The first used the well-known 1998 DARPA data sets. The sensors employed were the network-based Snort and the host-based STIDE. For each host session, all alerts generated by the two sensors were taken as a pattern. These patterns were than clustered, and a representative from each cluster was taken as a case for the case library. For this purpose a novel XML distance measure was created, to measure the distance between patterns in terms of their IDMEF representations. The clustering very effectively distinguished normal sessions containing false alerts from sessions containing real attacks, and in about half the latter cases, successfully identified the name of the attack. As mentioned, a key issue in meta-intrusion detection is alert correlation, i.e., determining when alerts generated by different sensors are a result of the same attack. The above employed what we have called *explicit* alert correlation, which makes use of IP addresses and other session information contained in the alerts.

The second experiment used the well-known 2000 DARPA data sets, which contain denial of service attacks spanning multiple host sessions. The data represents two different distributed denial-of-service (DDOS) attacks and gives all alerts in IDMEF. Here the original contribution has been a new *case-oriented* or *implicit* approach to alert correlation. The key idea here is to view a case as an example of correlated alerts. Then when a stream of alerts is generated during run time, this is examined dynamically to determine if any subsets of the alert stream match, or closely match, any cases in the library. Matches, or close matches, are interpreted as representing real attacks. The experiment showed that this approach can be very effective in detecting DDOS attacks.

The third experiment made use of an attack simulator known as the DARPA Grand Challenge Problem (GCP) program. This can simulate three different types of attacks (lifecycle, insider, and denial of service) against a fictitious shipping company. This experiment also used case-oriented alert correlation for matching subsets of the input alert stream with cases in the library. Again alerts are represented in IDMEF and the XML distance measure is applied. Two matching methods were explored, one based on the well-known Hungarian algorithm and one taking the temporal ordering of the alerts into account and employing dynamic programming. It was found that both methods are effective for attack detection and, in fact, produce almost identical results. The dynamic programming is preferable, however, in that it runs in linear time and is significantly more efficient.

In conclusion, we believe we have demonstrated that our proposed methodology actually works. Further effort will be required, however, to bring this to real-world applications. One pressing issue is the need for a generalized attack simulator, one that can simulate attacks of any of the currently known kinds against a network of arbitrary size and complexity. Such a simulator will be needed to generate case libraries for any arbitrarily given real-world organizations.

Human and organizational factors in computer and information security

The group led by P. Carayon at the University of Wisconsin-Madison has developed an understanding of the human and organizational factors involved in various facets of computer and information security (CIS). Our research has examined human and organizational factors in computer and information security. Current approaches to and remedies for CIS vulnerabilities do not take non-technical causes (i.e. human and organizational factors) into account in the development, implementation, and configuration of CIS systems. CIS problems are usually approached from a technology-centric viewpoint: current remedies are to build stronger technical defenses (e.g., stronger encryption methods, anti-virus software) in order to control and limit CIS vulnerabilities and breaches. Our research demonstrates that numerous non-technical factors can contribute to CIS performance and can impact the occurrence of CIS vulnerabilities. Human and organizational factors taken into consideration in the design, implementation, and operation of CIS systems will enhance the performance of CIS systems.

We developed three areas of research: (1) human factors methods of analysis in CIS; (2) the defenders' viewpoint of human and organizational factors in CIS; and (3) the adversarial viewpoint of human and organizational factors in CIS. Each of the three areas is discussed separately.

Human factors methods of analysis in CIS

We have developed two human factors methods of analysis for CIS. First, the Human Factors Vulnerability Analysis (HFVA) is a method for diagnosing human factors in CIS. HFVA is used in conjunction with a technical vulnerability audit, such as Nessus: it provides additional in-depth information on the human and organizational factors involved in specific technical vulnerabilities. HFVA has been pilot tested in collaboration with Dr. Mary Vernon's research team at the University of Wisconsin-Madison. The MS thesis of Sara Kraemer, research assistant, describes the development and pilot testing of the HFVA. Second, we have developed a conceptual framework of work system elements, human errors, and violations in CIS. We conducted semi-structured interviews with eight network administrators and eight CIS specialists to develop and refine this conceptual framework. The interviews provided data on the types of human errors and violations, as well as human factors and work systems errors related to human error. We have reported our conceptual framework and research findings in a peer-reviewed journal publication that will be published in *Applied Ergonomics* in 2006.

Defenders' viewpoint of human and organizational factors in CIS

In our second area of human factors research, we have examined human and organizational factors of CIS from the defenders' perspective. We have drawn parallels among the organizational functions of occupational safety and health (OSH), quality, and CIS. We have identified eight dimensions that can be used to describe and compare the organizational functions: tradeoffs, culture, tools and methods, policies and procedures, organizational structures, regulations and standards, audits, and outcomes versus processes. Managers of the CIS function can learn from 'best practices' that managers of the OSH and quality functions have developed over time.

We have developed a framework of human and organizational factor and CIS vulnerabilities from the defenders' perspective. We have submitted a paper on this framework: the paper summarizes the findings of a working group on *Human Factors in e-Security* that was organized in collaboration with Professor Veeramani and the E-Business Consortium of the University of Wisconsin-Madison. The paper is entitled: *Security Managers' View of Human and Organizational Factors in Computer and Information Security*, and was re-submitted to *Computers & Security* in January 2006. It presents a framework that links human and organizational factors to CIS vulnerabilities. Some key human and organizational factors include: CIS policy development, training of CIS practices and procedures, implications for the design of complex CIS systems, usability of CIS methods, such as passwords, and CIS culture.

We have also further examined a few specific areas of the defenders' viewpoint. For example, we developed a human factors understanding of CIS culture. We combined the findings of two separate data collection efforts (i.e. interviews with CIS managers and network administrators, workgroup) to describe the various dimensions of CIS culture: employee participation, training, hiring practices, reward systems, management commitment, and communication and feedback. This analysis resulted in a paper presented at the annual meeting of the Human Factors and Ergonomics Society in 2005.

Adversarial viewpoint of human and organizational factors in CIS

In our third area of human factors research, we examined human and organizational factors in CIS from the adversaries' perspective. The adversarial viewpoint of CIS consists of two research components: adversaries' perspective of human and organizational factors in CIS and the performance of red teams in CIS. We have developed these areas of research in collaboration with Sandia National Laboratories' Information Design Assurance Red Team (IDART™) program in Albuquerque, New Mexico.

The research in the adversarial viewpoint of human and organizational factors in CIS investigated the nature of possible non-technical causes of poor performance of CIS systems and CIS vulnerabilities. This research was the topic of Sara Kraemer's Ph.D. thesis (title: *An Adversarial Viewpoint of Human and Organizational Factors in Computer and Information Security*). The objectives of this study were to: (1) identify and describe the various human and organizational factors associated with CIS and (2) describe how human and organizational factors and their associated mechanisms contribute to technical CIS vulnerabilities. This research used red teams at the IDART™ program as a source of data. Fourteen red team members in individual interviews reported 589 total comments on the types of human and organizational factors consistent with the categories of the work system model developed by Carayon and Smith (1989; 2000). The human and organizational factors consist of the following categories: organization (372 comments), individual (124 comments), task (46 comments), technology (40 comments), and environment (7 comments). Two focus groups of five red team members constructed the various mechanisms and pathways of specific human and organizational factors related to specific types of CIS vulnerabilities: design,

implementation, configuration, and operational vulnerabilities. Information from this research will be used by the Sandia IDART™ program to improve their approach to the analysis of CIS.

In the area of red team performance, we conducted a study to examine the various team components and processes that contribute to and hinder a high-performing red team. In addition, we have developed a set of red team performance metrics. Lastly, we performed a trade-off analysis comparing and contrasting red team performance to technical modeling/simulation techniques. We have re-submitted a paper on red team performance to *Human Factors* in November 2005.

Resilient system architectures

Analytical framework for robust and resilient systems

The research group at The George Washington University had as its overall goal the development of analytical frameworks for design and analysis of robust and resilient critical infrastructure systems. To address this goal, we have concentrated on characterization of vulnerabilities, assessment of threat and risk analysis in interacting networked systems. Specific tasks included

- Design of robust tools for information aggregation and fusion, and representation and management of uncertainty,
- Development of a rigorous framework for modeling and analysis of failures, and optimization of performance in networked interacting systems containing uncertainties at different levels,
- Development of consistent models for cascading failures, and dynamic analysis of interdependent infrastructures, and
- Reliability analysis of networked systems, including dynamic reliability analysis of totally mobile network architecture.

Reliability of networked systems

Realistic assessments of the reliability of networked systems require accounting for the interdependence between the lifetimes of different components. This requires use of a multivariate probability distribution, several of which have been proposed in the literature. In our work, we have identified ways in which users can express dependence, and introduce a family of multivariate distributions that makes it possible to assess degrees of dependence that are not easily modeled using other distributions

It can be argued that dependencies between the nodes of a network or the components of a system can be attributed to commonalities in the unit's "genetic" makeup (for example, commonalities of design and manufacturing), among other things. Sharing a common environment is another source of dependencies, but this is not considered here (see "stability of networked dynamical systems"). We are able to show that multivariate exponential distributions, with unit exponentials as marginal distributions, capture the nature of this genetic dependence. We call each marginal exponential the "hazard potential of the unit." Dependent life lengths are a consequence of the rate at which the hazard potential is depleted. Thus, to generate multivariate life lengths, we must have

unit multivariate exponentials as a seed. "Copulas" are a way of generating multivariate distributions with specified forms of dependence. We are currently pursuing work linking the idea of copulas with the notion of hazard potentials to generate multivariate life distributions with specified dependencies.

Representation and quantification of uncertainty

The representation and quantification of uncertainty is pivotal to modeling frameworks for infrastructure systems. The notion of fuzzy sets has proven useful in the context of control theory, pattern recognition, and medical diagnosis. However, it has also spawned the view that classical probability theory is unable to deal with uncertainties in natural language and machine learning, so that alternatives to probability are needed. One such alternative is what is known as "possibility theory". Such alternatives have come into being because past attempts at making fuzzy set theory and probability theory work in concert have been unsuccessful. We have developed a line of argument that demonstrates that probability theory has a sufficiently rich structure for incorporating fuzzy sets within its framework. Thus probabilities of fuzzy events can be logically induced. The philosophical underpinnings that make this happen are a subjectivist interpretation of probability, an introduction of Laplace's famous genie, and the mathematics of encoding of expert testimony. The benefit of making probability theory work in concert with fuzzy set theory is an ability to deal with different kinds of uncertainties that may arise within the same problem. In this effort, we also relate to other methods of uncertainty quantification.

Resilience of mobile wireless architectures

Our collaborators at the University of Central Florida have developed recovery protocols for hybrid mobile wireless architectures that combine the advantage of ad-hoc (mobile nodes) and cellular models. Such architectures provide an essential ingredient for "communication-on-the-move" service in dynamic battle space with enhanced flexibility and stability. In order to ensure reliability and robustness of such systems, we have investigated the resiliency of such architectures by considering strategies for optimal deployment (number and location) of back-up routers that would ensure reliable performance in such interdependent mobile systems.

Basically, in this architecture, specialized mobile routers (usually placed in moving trucks) are used to achieve continued connectivity and fast message forwarding. Satellite links or backbone wireless channels are used for communication between each mobile router, while short-hop wireless channels are used for communication between each mobile router and its users (mobile hosts). When mobile hosts move, the mobile routers also move (following certain dynamic path) to ensure the continuity of coverage and improve the quality of service for active connections.

What happens if any of the mobile routers fails, either due a natural hazard or a malicious attack? In order to overcome such exigencies and design fault-tolerant architectures of mobile routers, the network of routers could be equipped with robust fault-tolerant and recovery protocols. These protocols normally entail adding redundant hardware and (back-up) routers, requiring extra overhead for achieving satisfactory operations. The

cost-benefit analysis for enhancing reliability and resilience in such mobile architectures presents some challenging technical problems. Specifically, we consider the development of strategies for optimal deployment (number and location) of back-up mobile routers that achieve enhanced reliability and resilience in the overall performance of mobile architecture. While in this paper, our primary focus has been on explicit strategies that can be implemented for multiple primary routers that are relatively stationary, our current and future work will consider moving primary routers under various mobility models (both deterministic and stochastic).

Stability of network-centric dynamical systems

Many infrastructure systems such as power grids, transportation systems, and communication networks (and the interdependencies among them) can be modeled as stochastic hybrid dynamical systems. Stability analysis of such models enables one to assess the dynamic reliability and resilience of such complex systems with respect to various exogenous factors. We have investigated stability of such network-centric dynamical systems that might be subject to external disturbances and/or structural perturbations.

The primary motivation for this work comes from the need to develop predictive models of various failure modes in such complex interacting dynamical systems. We are also interested in the assessment of reliability and performance under dynamic environments. With this in mind, we intend to pursue some related control problems utilizing the framework developed in this paper. Also, dynamic reliability of such complex network systems is of considerable practical interest for the assessment of robust and resilient performance under both stochastic disturbances and structural degradation.

Reliability optimization for interconnected components

A key aspect of engineering design is the attainment of high reliability. For a system of interconnected components, like a network, high reliability is achieved in one of two ways: by increasing the reliability of each component or by introducing redundant components. Either strategy entails costs, thus design problem boils down to optimizing reliability subject to cost constraints. Such reliability allocation problems have been considered before, but the focus has been on allocating redundancies rather than reliability. Attempts at the latter topic suffer from a drawback, namely, that component interdependencies have not been considered. In our work, we have overcome this drawback, and provided a foundation for addressing a class of optimization problems in reliability.

Resource allocation under risk

V. M. Bier and her students (together with other colleagues as co-authors) have addressed a number of aspects of resource allocation for homeland security. Building on the initial paper by Bier, Nagaraj, and Abhichandani, topics that have been addressed to date include:

- The effects of system structures (including structures more complex than simple series and parallel systems)
- The effects of uncertainty about attacker goals and asset valuations
- The effects of discrete investment options (rather than continuous investment levels)

- The merits of investing in protection from natural disasters versus terrorism
- The effects of security investments on the incentives for investment faced by other agents
- The effects of discount rates on security investments
- The roles of disclosure, secrecy, and deception in achieving optimal security
- The relative merits of "overarching" defenses (such as border security, emergency preparedness, intelligence gathering, or public health) compared to target hardening

In related work, Bier has also written or co-authored a book chapter on the bureaucratic and organizational failures in the preparation for and response to Hurricane Katrina, two articles on the use of expert opinion in risk analysis, an article on vulnerability assessment for electrical transmission networks, and an article on human factors in computer security (co-authored with Carayon).

The paper [2] on optimal allocation of security investment in series and parallel systems (Bier with Abhichandani and Nagaraj) clearly illustrated how protecting targets against intentional attacks differs from protecting against accidents or acts of nature. In other words, the paper showed the difficulty of defending series systems from intelligent attack, and highlighted the importance of redundancy as a defensive strategy. In particular, the paper showed that redundancy increases defender flexibility (i.e., the defender's ability to allocate defensive resources to targets according to the cost effectiveness with which they can be defended), and reduces attacker flexibility. The model developed in this paper paved the way for rigorous mathematical study of optimal security investment in a wide range of circumstances.

As one example of such work, the paper [153] on the effects of uncertainty (Bier with Samuelson and Oliveros) was described as "path breaking work" by the associate editor handling that manuscript. The most noteworthy feature of this work was that it showed that excessive investment in one target could actually worsen overall levels of security in some contexts, by deflecting attacks from the over-protected target to other targets that were more valuable and/or less well defended, thus causing greater expected damage. This paper also showed that even in the face of uncertainty about attacker goals and motivations, it will often still be optimal to leave some targets undefended, even if they have a non-zero probability of being attacked. This is especially likely to be true when targets vary widely in their values, and when the defender is highly resource-constrained—conditions which will frequently be satisfied in practice.

The results of this body of work could eventually be implemented in "portfolio management" software for facility security improvement. Such software would incorporate some features of traditional budget allocation (choosing investments according to their cost-effectiveness, where appropriate), but also take into account the series/parallel structure of the system to be defended, using simple game-theoretic models of the likely attacker response to particular investments.

Stochastic optimization methods for networked systems

The work of this grant, and many other tasks of importance to DOD as well, involves finding ways to improve or optimize the performance of networked, interacting systems containing significant uncertainties. Given a limited budget for improving the performance of such a system, how should it be allocated to give the best improvement? One of the most useful tools in analyzing such systems is stochastic simulation, but if one wants to improve the system, rather than just to predict its performance "as-is," then repeated simulations are usually necessary. If the system is complex, these simulations often require long running times, and therefore such analyses can require very large amounts of time.

The group led by S.M. Robinson at UW-Madison developed a two-phase approach, with the aim of improving or optimizing the network in much less time. The first phase uses stochastic network approximations in place of repeated simulations to predict good ways to improve the network's performance, while the second phase uses one simulation run to validate the predicted improvement. Tests on a variety of networked systems, including some arising in military logistics, have shown that the method works very quickly (time reductions of 96%-98% are not unusual), with good accuracy.

Analytical tools for variational conditions

Many models of interest in this research program, including Nash equilibrium models arising from game-theoretic settings, can be written as *variational conditions.* Such a condition makes precise the intuitive geometric idea of a normal to a set at one of its points. This idea is quite simple when the boundary of the set is smooth, but in important applications this smoothness property often fails. When that happens, the variational condition formalism gives a satisfactory way of extending the intuitive idea to the more general situation.

A particular example of a variational condition is user equilibrium in a transportation network. Transportation networks are important components of infrastructure. To predict the travel patterns in, and therefore the performance of, such networks people often use the Wardrop equilibrium conditions to compute an equilibrium flow in the given network for a prescribed set of demands for travel between origins and destinations.

Because these models appear in so many places, it is of great interest to have analytical tools for studying them and for analyzing the sensitivity of their solutions. These tools are the analogues for variational conditions of the standard implicit-function theorem for smooth equations.

In [19], Robinson studied the sensitivity analysis of variational conditions defined over perturbed systems of finitely many nonlinear inequalities or equations, subject to additional fixed polyhedral constraints. If the system of constraints obeys a certain property called *nondegeneracy*, he showed how to construct a local diffeomorphism of the feasible set to its tangent cone. Moreover, this diffeomorphism varies smoothly as the perturbation parameter changes. The original variational condition is then locally equivalent to a variational inequality defined over this (polyhedral convex) tangent cone.

This result extends stability results already known for variational inequalities over polyhedral convex sets to a substantially more general case. The paper also shows that existence, local uniqueness, and Lipschitz continuity, as well as B-differentiability of the solution can all be predicted from a single *affine* variational inequality that is easily computable in terms of the data of the unperturbed problem at the point in question.

A specific example of the applicability of the theory in the nondegeneracy paper is the convergence analysis of fast methods for solving variational conditions. Robinson analyzed in [22] a linearization method that provides an analogue of Newton's method for numerical solution of variational conditions. Further tools for stability analysis of variational conditions appear in [21]; the assumptions required here are much weaker than those required for nondegeneracy, but they still yield useful information about the existence and stability of solutions.

Robinson also prepared by invitation a survey paper [20] covering analytical methods for variational conditions with smooth constraints. This is the archival version of an invited semi-plenary address at the triennial International Symposium on Mathematical Programming, held in Copenhagen, Denmark in August 2003.

Finally, in very recent work [170] Lu and Robinson extended known techniques for the analysis of sensitivity and stability to variational inequalities posed over polyhedral convex sets in which the right-hand sides of the inequalities and equations defining the sets may vary. These techniques were not previously available for problems with right-hand side variations.

Rapidly deployable mobile networks

The research group led by Mostafa Bassiouni at the University of Central Florida developed and evaluated a two-tier rapidly deployable mobile network model. This wireless network model is based on a hybrid ad-hoc cellular network architecture that replaces the stationary cellular base stations with mobile routers. The specialized mobile routers are used to achieve continued connectivity and fast forwarding. A mobile router has functionality similar to a cellular base station, but has no wired connections. In its simplest form, the mobile router could be a truck-mounted transceiver box with rechargeable battery. Our hybrid network model provides "communications-on-the-move" services with enhanced flexibility and scalability. Communications among the mobile routers is achieved using satellite links or high bandwidth wireless channels. Our detailed simulation tests have shown that improved performance and increased reliability can be obtained by arranging the mobile routers into a hierarchy of two levels. Routers at the lower level have a standard range of coverage and are devoted to servicing individual groups of users (called swarms). Routers at the higher level have a larger transmission range and are used to provide "umbrella" coverage for multiple swarms. By tuning the power level of their transmitter, the mobile routers can adjust their range of coverage and switch from one level of the hierarchy to the other. The following are the two areas of investigation related to our hybrid wireless network model.

Backup recovery protocols

A mobile router can become immobilized due to a flat tire, failed automotive engine, or some type of road obstruction. Although the mobility of the router is compromised, the wireless transceiver in this case is intact and can continue to provide service in a stationary mode. A more serious scenario is the failure or total destruction of the router's transceiver. This condition forces the termination of all active connections served by the failed router. In order to be able to handle these faults when they occur, the network must be equipped with robust fault tolerance and recovery protocols. These protocols normally entail adding redundant hardware and incurring some extra overhead during normal operations. We have designed and evaluated two types of recovery protocols: the dual backup protocol and the distributed recovery protocol.

We evaluated the dual backup and the distributed recovery protocols using a detailed simulation model. The simulation prototype has 36 active mobile base stations serving 1800 mobile terminals. The number of standby stations in the simulation is changed from zero (i.e., no recovery) to 36 (i.e., the number of active stations). Different values are used for MTBF (mean time before failure) for active and standby stations. Numerous simulation experiments have been used to obtain performance for the following cases: a) degradation tests, b) steady-state performance, and c) comparison of recovery for the two-tier and the single tier architectures. The dual backup protocol has been found to be simple and to provide definite performance gains in face of hostile attacks and threat conditions. In particular, the dual backup protocol provides the fastest recovery when a backup router survives the destruction of its primary router. In general, however, the distributed recovery protocol has given better performance especially in the case when failed stations can be repaired and put back into service after some repair time. Our simulation tests have also shown that the second-tier architecture further improves the performance of the distributed recovery protocol. Finally, we have developed an analytical model for the distributed recovery protocol and verified its accuracy by simulation.

Location-based routing

We have also designed and evaluated an efficient location–based routing (LBR) protocol for our rapidly deployable mobile network model. The LBR protocol is based on using mobile positioning services and requires each mobile router to exchange its position information only with its neighboring mobile routers. Compared with an ideal flooding-based routing algorithm, our LBR protocol greatly reduces the number of hops visited during the search process, while ensuring that routers are still highly reachable. Consequently, our LBR algorithm achieves a routing success rate that is very close to that of the flooding approach but with significant reduction in power and bandwidth consumption. When a mobile router C receives a message destined to mobile router D, it forwards the message to the neighbor that has the highest routing weight. If N is a neighboring mobile router of the current mobile router C, the routing weight of N is based on three factors: 1) the estimated gained distance toward the destination D, i.e., the length of the projection of vector CN on the vector CD, 2) the useful degree of N, i.e., the number of neighbors of node N that seem able to further drive the search nearer to D, and 3) the deviation angle of N, i.e., the angle between vector CD and vector CN. We

conducted extensive simulation tests to evaluate the performance of LBR. The number of mobile routers in our tests ranged from 20 to 70. The tests showed that the proposed LBR algorithm greatly reduces the number of hops visited during the search while incurring extremely small reduction in reachability.

Linear traffic predictor with dynamic error compensation

We have developed and validated a new linear prediction scheme for Internet traffic. We started our research by performing extensive performance comparisons of three known predictors: 1) Gaussian, 2) auto-regressive moving average (ARMA) and 3) fractional auto-regressive integrated moving average (fARIMA). Based on the results of these tests, we proposed and evaluated a new traffic predictor with dynamic error compensation, L-PREDEC.

Our comparison tests among the three traffic prediction algorithms (Gaussian, ARMA, and fARIMA) were based on the mean packet delay, the variance of the packet delay, and the buffer requirements. Our tests used a collection of real-life traffic traces including packet header traces collected in 2002 by the National Laboratory for Applied Network Research (NLANR) and the Auckland-6 traces collected in 2002 from the Auckland Internet access path by the WAND group at the University of Auckland, New Zealand. Our performance tests using the above traffic traces have shown that L-PREDEC has an improved response time to bursty traffic and works better than Gaussian, ARMA and fARIMA in terms of the three metrics listed above. We discussed one application of L-PREDEC, namely, the development of efficient dynamic link resizing schemes that can be used to get multiplexing gain without QoS degradation in Internet access paths and in virtual private networks.

Temporal failure and degradation

We have designed an approach for modeling and analyzing the temporal failure and degradation behavior of critical infrastructure systems (CISs) using advanced temporal database management systems. We classify the possible failure and/or degraded performance of CISs into different temporal categories, namely, crisp or exact intervals, non-vanishing imprecise intervals and vanishing imprecise intervals. The three temporal operators: Union (OR), Overlap (AND) and Not are extended to operate on the above categories of precise and imprecise intervals. The temporal operators are used recursively to capture the fault tolerance topology of CIS. For example, if a component of CIS has built-in redundancy for fault tolerance, the fault behavior of this component propagates to the outside only when all the redundant units of this component fail simultaneously. In this case, the *failure temporal expressions* of the redundant units are joined by temporal Overlap operators to indicate that the failure of the composite component is contingent on the failure of all units. We investigated how query languages with temporal extensions can be used to obtain useful answers for time-related queries and retrieve useful information about the exact and potential time points for degraded modes of operation. We also analyzed the storage overhead of incorporating the imprecise intervals in a temporal database.

Optical communications networks

Optical wavelength-division multiplexed (WDM) networks are rapidly becoming the technology of choice in network infrastructure and next-generation Internet architectures. We have designed and evaluated new schemes for 1) path protection in survivable optical networks, 2) real-time routing and channel assignments in multi-fiber optical networks, and 3) supporting differentiated quality of service in optical burst switched networks. The following is a high-level summary of the results in the three topics of the optical communications networks area.

Alarm-based path protection in survivable WDM optical networks

We have designed and tested a new alarm-based path-protection scheme with routing and path-selection processes that take into consideration the alarms posted for the various links and nodes of the network. The goal of the scheme is to improve the reliability of the network and reduce service outage. We compared our scheme with 1) the greedy Dedicated Path Protection (DPP) scheme, 2) the capacity-efficient Disjoint Shared Path Protection (DSPP) scheme and 3) the Joint Shared Path Protection (JSPP) scheme. Our extensive simulation results have shown that our alarm-based scheme outperforms the above three schemes in terms of loss-of-service ratio and network throughput. The simulation tests used a wide range of values for the load intensity, the failure arrival rate, and the failure holding time. We also extended our path protection scheme to the differentiated services model. The extended quality-of-service (QoS) enhanced scheme uses preemption to minimize the connection blocking percentage for high-priority traffic. The scheme handles the flowing four classes of connections in ascending order of priority: 1) Preemptible with no protection, 2) Preemptible with shared protection, 3) Non-preemptible with shared protection, and 4) Non-preemptible with guaranteed protection. Our extensive simulation results have shown that the enhanced scheme can achieve a clear QoS differentiation among the four traffic classes and at the same time provide good overall network performance.

Real-time routing and channel assignment in multi-fiber optical networks

We designed and evaluated a new approach for implementing efficient routing and wavelength assignment (RWA) in WDM optical networks. In our method, the state of a fiber is determined by the set of free wavelengths in this fiber and is efficiently represented as a compact bitmap. The state of a multiple-fiber link is also represented by a compact bitmap computed as the logical union of the individual bitmaps of the fibers in this link. Likewise, the state of a light path is represented by a similar bitmap computed as the logical intersection of the individual bitmaps of the links in this path. The count of the number of 1-valued bits in the bitmap of the route from source to destination is used as the primary reward function in route selection. We modified the Dijkstra algorithm and used it for dynamic routing based on the compact bitmap representation. We also developed a first-fit channel assignment algorithm using a simple computation on the bitmap of the selected route. The resulting routing and channel assignment scheme uses fast bitwise logical operations and is quite efficient. It combines the benefits of least loaded routing algorithms and shortest path routing algorithms. Our extensive simulation

tests have shown that the bitwise RWA approach has small storage overhead, is computationally fast, and reduces the network-wide blocking probability.

Supporting differentiated QoS in optical burst switched networks

We have developed and evaluated two new schemes for providing differentiated services in optical burst switched (OBS) networks. The first scheme adjusts the size of the search space for a free wavelength based on the priority level of the burst. A simple equation is used to divide the search spectrum into two parts: a base part and an adjustable part. The size of the adjustable part increases as the priority of the burst becomes higher. The scheme is very easy to implement and does not demand any major software or hardware resources in optical cross connects. The second scheme reduces the dropping probability of bursts with higher priorities through the use of different proactive discarding rates in the network access station (NAS) of the source node. Our extensive simulation tests using just-in-time (JIT) signaling have shown that both schemes are capable of providing tangible QoS differentiation without negatively impacting the throughput of OBS networks.

Fair sharing of bandwidth in distributed local area networks (LANs)

Fair sharing of bandwidth in distributed systems is a challenging issue and it has been researched extensively. By fairness, it is meant that users get resources proportional to their weightings. There are two main problems in achieving fair share of bandwidth in distributed systems: lack of information and lack of coordination. Lack of coordination is more fundamental because even if the users have complete information about the other users, their transmission activities cannot be coordinated to achieve fairness. We have modeled this contention-based nature of medium access using non-cooperative game theory and analyzed the system accordingly. We have proposed a Medium Access Control (MAC) protocol along the lines of *p*-persistent Carrier Sense Multiple Access (CSMA). Users compute their optimal transmission probabilities such that their payoff functions are maximized. We consider two game-theoretic solution concepts for computing the transmission probabilities: Nash Equilibrium (NE) and Constrained Nash Equilibrium (CNE).

We have modeled the distributed medium access as a non-cooperative game; designated as the Access Game. Nash Equilibrium (NE) and Constrained Nash Equilibrium (CNE) were proposed as solutions for the Access Game. NE does not necessarily result in fair sharing of the bandwidth. Therefore, CNE was proposed as a solution.
CNE results in fair sharing of bandwidth amongst competing users. However, the existence of CNE depends on all the users adhering to the fairness constraints. However, one or more users may decide to cheat and break these constraints. This results in instability in the system. In order to tackle this problem, we use NE.

NE for the Access Game is unique in nature and hence, stable. Therefore if the NE of the Access Game results in fairness, then we achieve both bandwidth fairness and system stability. We have proven that there is unique operating point in the system such that fairness is satisfied and throughput is maximized. We propose to design the system in such a way that the NE corresponds to this operating point.

We have proposed two techniques to this effect. One technique chooses the weightings of the users suitably and the other technique deploys a punishment mechanism to penalize users transmitting with higher rates. Our results show that these techniques achieve the desired objective.

Java middleware for parallel programming in SMP and heterogeneous clusters

Cluster computing provides a cost-effective parallel computing platform as a network of PCs or workstations. Clusters are normally built up with commodity-off-the-shelf (COTS) hardware components, free or widely used software like Linux, Windows NT, and a variety of middleware libraries. Parallel programming libraries provide necessary programming tools to develop parallel programs over the cluster. Message passing programming models and libraries have been most widely used in cluster computing, where each node executes a different stream of instructions and exchange messages when they need to share data or coordinate with other nodes. Message Passing Interface (MPI) has been used as a de facto standard for message passing based parallel computing. MPI specifies the necessary point-to-point and advanced collective communication primitives for message passing. MPI and other message passing libraries such as Parallel Virtual Machine (PVM) have been widely used in developing parallel applications, proving its effectiveness due to simplicity and portability over various parallel computing platforms.

A new programming language, Java, and its associated technologies opened a door to more efficient development of distributed computing software, due to its built-in thread support, platform neutral byte codes, concurrent programming model based on the *monitor* concept, object oriented, and inter-process communication mechanisms such as TCP/IP sockets and Remote Method Invocation (RMI). Recently, Java has also enforced its viability as a distributed computing tool by incorporating Java cryptography and security packages as a part of recent JDKs. The objective of this project is to develop a Java based middleware (environment) for efficient development of parallel and distributed computing software. We have developed a new parallel programming model based on threads and implemented this model in Java.

A basic computing unit in VCluster is a communicating virtual thread, which is built on Java thread. Communication sources are associated with an individual thread instead of processes in conventional libraries to facilitate the communication between threads. Computation data is stored in virtual states that are associated with threads. Deprecating computation data from threads makes it easy to implement thread migration.

The architecture is implemented purely in Java. Problem of heterogeneity is solved by utilizing the unparallel portability of Java. Techniques like multithreading, object serialization, Java NIO, and separate send/receive threads are used to implement and improve the performance of the basic system.

Several applications, including communication latency test, Dirichlet problem, back propagation neuron network, and molecular dynamics simulation, have been developed in

VCluster and MPICH, mpiJava, jPVM to evaluate the performance of VCluster. The experimentation results show that the performance of VCluster is close to other Java libraries.

We also experimented with multithreading to utilize the full power of clusters of SMP machines. Since MPICH does not support multithreading, we combined MPICH with threading libraries like PThread and OpenMP. mpiJava and jPVM use Java threads. Our programming experience shows that developing multithreading applications in VCluster is significantly easier than in MPICH or other Java libraries. The experimentation results also show that VCluster provides close performance to C libraries.

In the development of molecular dynamics simulation, we implemented thread groups and collective communication functions between threads in a group. Collective communication has been proven to be very useful in MPI. However, collective communication between threads is very difficult to be implemented under the MPI architecture, which defines communication between processes instead of threads.

We have implemented thread migration and a very basic load balancing algorithm. We plan to implement load balancing based on thread migration.

Data distribution management for High Level Architecture

Data Distribution Management (DDM) is responsible in distribution simulation for limiting and controlling the data exchanged in a simulation and reducing the processing requirements of federates. DDM is also an important problem in the parallel and distributed computing domain, especially in large-scale distributed modeling and simulation applications, where control on data exchange among the simulated entities is required. In this work we plan to develop a new DDM algorithm.

We have developed a new algorithm, called *P-Pruning algorithm*, for the data distribution management problem in High Level Architecture. We also conducted a performance-evaluation simulation study of the P-Pruning algorithm against three other DDM techniques: region-matching, fixed-grid, and dynamic-grid algorithms. The *P-Pruning* algorithm is faster than region-matching, fixed-grid, and dynamic-grid DDM algorithms as it avoids the quadratic computation step involved in these algorithms. By populating the multicast group, first only on the basis of X-axis information of routing space, and pruning the multicast groups of non-overlapping subscriber regions in another step, it avoids the computational overheads of other algorithms. The performance evaluation results show that the *P-Pruning* DDM algorithm is faster than the three DDM algorithms, uses memory at run-time more efficiently, and requires less number of multicast groups. We have also extended the *P-Pruning* algorithm for dynamic conditions to allow federates join and leave federation at run-time. We also enhanced the *P-Pruning* algorithm to a three-dimensional routing space environment and proposed its possible deployment in multi-dimensional routing space. Our theoretical contributions include the average-case computational complexity analysis of the *P-Pruning* algorithm and its comparison with the three DDM methods: region-matching, fixed-grid, and dynamic-grid

algorithm. We have also analyzed the effect of changes in the distribution of federates within the routing space on the *P-Pruning* algorithm.

In high-performance distributed simulation, system scalability can be seriously inhibited by limits on resources such as communication bandwidth, memory, and CPU availability. To increase the scalability of *P-Pruning* algorithm, we developed a resource-efficient enhancement for the P-Pruning algorithm. We also conducted a performance evaluation study of this resource-efficient algorithm in a memory-constraint environment. The *Memory-Constraint* P-Pruning algorithm deploys I/O efficient data-structures for optimized memory access at run-time. The simulation results show that the *Memory-Constraint P-Pruning* DDM algorithm is faster than the P-Pruning algorithm and utilizes memory at run-time more efficiently. It is suitable for high performance distributed simulation applications, since it improves the scalability of the P-Pruning algorithm by several orders in terms of the number of federates. We have integrated the P-Pruning algorithm with the FDK software. FDK is an implementation of HLA architecture developed by the Georgia Institute of Technology. In the near future, we plan to develop scalable, resource-efficient distributed DDM techniques with implementation on cluster computers. We also plan to enhance the FDK software by implementing it on a distributed environment based on cluster computers.

Improving quality of service in 802.11e wireless LANs

IEEE Standard 802.11e is currently being developed to introduce Quality of Service (QoS) requirements in Wireless LAN (WLAN), so that it can overcome the shortcomings of the legacy 802.11. 802.11e provides QoS based on traffic categories. In this work, we consider how to provide better QoS for 802.11e MAC protocol in WLAN. We suggest some enhancement to current MAC 802.11e protocol that will be able to provide QoS depending on the class to whom a node belongs to in addition to the traffic category used by the node. Various tradeoffs can be provided in our suggested solution depending on the importance of objective function: bandwidth utilization or prioritization of node's ability to transmit.

In this work, we suggest an enhancement to the MAC layer protocol as an effort towards a more reliable service to nodes registered to receive QoS. Nodes are assured transmission opportunities within their delay bounds in the contention free period (CFP). A beacon is used to mark the start of a CFP. Any delay in the issuance of the beacon would adversely affect the timely delivery of time-sensitive traffic. In IEEE 802.11e beacon delays affect negotiations between the access point and the registered nodes. We propose a scheme that prevents the delays in beacon issuance, which are caused due to nodes operating in the contention period, transmitting MAC service data units beyond super frame boundaries. Our beacon management scheme not only assures a timely beacon issuance thus enhancing the delay guarantees but also maintains the throughput. Simulations were conducted to analyze the performance of the proposed scheme. The results demonstrate that when timely transmission of QoS bound traffic is achieved by preventing a late beacon issuance, the average length of super-frames is maintained and results in increased number of super frames over time indicating that registered nodes would get longer amounts of time to transmit data if such delays are prevented.

Integration, synthesis and impact

A simulation test-bed for network based systems

The group led by Ratan Guha at UCF worked to design a parallel simulation test-bed for a critical infrastructure. Since most critical infrastructures are networked based systems, our goals are to reduce redundant software design efforts in the area of simulation of network based systems, establish a framework general enough to be used for the simulation of many network-related technologies, and provide for a common base for the experimentation of various security infrastructures. The object-oriented nature and the use of a popular programming language for implementation allow researchers to easily modify, reuse and share whole systems or system components. The architecture should also include customizable user interface that can be easily adapted to a specific problem via code. A very clean graphical environment allows the system to be used for demonstrational or educational purposes. The GUI can be executed separately from the simulation engine and can function as a visual demonstration of an algorithm or a system.

We have developed a portable, open-source Parallel Interactive Network Simulation (PINS) framework specializing in simulations of wireless network infrastructures. This development is based on a modular architecture of the simulation framework and applied to the studies of mobility pattern effects, routing and intrusion detection mechanisms in simulations of large-scale wireless ad hoc, infrastructure, and totally mobile networks. The distributed simulations within the framework execute seamlessly and transparently to the user on a symmetric multiprocessor cluster computer or a network of computers with no modifications to the code or user objects. The visual graphical interface precisely depicts simulation object states and interactions throughout the simulation execution, giving the user full control over simulation in real time. Network configuration is detected by the framework, and communication latency is taken into consideration, when dynamically adjusting the simulation clock, allowing the simulation to run on a heterogeneous computing system. The simulation framework is easily extensible to multi-cluster systems and computing grids. An entire simulation system can be constructed in a short time, utilizing user-created and supplied simulation components, including mobile nodes, base stations, routing algorithms, traffic patterns and other objects. These objects are automatically compiled and loaded by the simulation system, and are available for dynamic simulation injection at runtime.

Using our distributed simulation framework, we have studied modern intrusion detection systems (IDS) and assessed applicability of existing intrusion detection techniques to wireless networks. We have developed a mobile agent-based IDS targeting mobile wireless networks, and introduced load-balancing optimizations aimed at limited-resource systems to improve intrusion detection performance. Packet-based monitoring agents of our IDS employ a CASE-based reasoning engine that performs fast lookups of network packets in the existing SNORT-based intrusion rule set. Experiments were performed using the intrusion data from MIT Lincoln Laboratories studies, and executed on a cluster computer utilizing our distributed simulation system.

Listing of all publications and technical reports supported under this grant

Papers published in peer-reviewed journals

1. V. M. Bier, Implications of the research on expert overconfidence and dependence. *Reliability Engineering and System Safety,* Vol. 85, pp. 321-329, 2004
2. V. M. Bier, A. Nagaraj, and V. Abhichandani, Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries, *Reliability Engineering and System Safety,* Vol. 87, pp. 313-323, 2005
3. J. Chandra and G. Ladde, Stability analysis of stochastic hybrid systems, *Intern. J. Hybrid Systems,* vol.4, no.1-2, p.179-198, 2004
4. J. Chandra, Z. Lu, and L. Shieh, Tracking control of nonlinear system: A sliding mode design via chaotic optimization, *Intern. J. of Bifurcation and Chaos,* 14, p.1343-1355, 2004
5. J. Chandra, A framework for robust and resilient critical infrastructure systems, *J. Adv. Computational Intelligence and Intelligent Informatics,* 10, p.265-269, 2006
6. J. Chandra, Z. Lu, L. Shieh, and G. Chen, Identification and control of chaotic systems via recurrent high-order neural networks, *Intelligent Automation and Soft Computing,* vol. 12 p1-17, 2006
7. J. Chandra and J. Landon, Towards a reliable and resilient mobile wireless architecture, *J. Stochastic Analysis and Applications,* **24**, 1-15, 2006
8. W. Cui and M. Bassiouni, Analysis of Hierarchical Cellular Networks with Mobile Base Stations, *Journal of Wireless Communications and Mobile Computing* 2, 131-149, 2002
9. W. Cui and M. Bassiouni, Virtual private network bandwidth management with traffic prediction. *Journal of Computer Networks* 42, 765–778, 2003
10. M. El Houmaidi, M. Bassiouni and G. Li, Alarm based Routing and Path Protection in Survivable Wave length Routed All-Optical Mesh Networks, *Journal of Optical Networking,* Optical Society of America, Vol. 4, pp. 176-190, March 2005
11. M. El Houmaidi and M. Bassiouni, Dependency Based Analytical Model for Computing Connection Blocking Rates and its Application in the Sparse Placement of Optical Converters, *IEEE Transactions on Communications,* Vol. 54, No. 1, pp. 159-168, 2006
12. M. El-Houmaidi, O. Kachirski and R. Guha, FANS Simulation of Optical Burst Switching for NSFNET, *WSEAS Transaction on Computers,* Volume 3, Issue 5, pp 1232 – 1237, Nov. 2004
13. J. Falk, N. Singpurwalla, and Y. Vladimirski, Reliability Allocation for Networks and Systems , *SIAM Review* Vol. 48, No. 1, pp. 43-65, 2006
14. J. Granger, A. Krishnamurthy, and S.M. Robinson, Rapid improvement of stochastic networks using two-moment approximations, *Mathematical and Computer Modelling* 43, 1038-1060, 2006
15. R. Guha and S. Rakshit, Selfish Users and Distributed MAC protocols in Wireless Local Area Networks (WLANs), *International Journal of Enterprise Information Systems (IJEIS),* Vol. 2, No. 2, pp 28 – 44, April – June 2006

16. Long, J., Schwartz, D., and Stoecklin, S., Multi-sensor network intrusion detection: a case-based approach, *WSEAS Transactions on Computers,* 4, 12, 1768-1776, 2005
17. S. Muhammad, R. Guha, and Z. Furqan, A Dynamic Simulation Model and Testing Techniques for Security Protocol Verification, WSEAS Transaction on Computers, Volume 3, Issue 5, pp 1226 – 1231, Nov. 2004
18. S. Rakshit and R. Guha, Fair Bandwidth Sharing in Distributed Systems: A Game-Theoretic Approach, IEEE Transactions on Computers, Vol. 54, No. 11, pp 1384 - 1393, 2005
19. S. M. Robinson, Constraint nondegeneracy in variational analysis. *Mathematics of Operations Research* 28, 201–232, 2003
20. 16. S. M. Robinson, Variational conditions with smooth constraints: Structure and analysis. *Mathematical Programming* 97, 245–265, 2003
21. S. M. Robinson, Localized normal maps and the stability of variational conditions. *Set-Valued Analysis* 12, 259 – 274, 2004
22. S. M. Robinson, A linearization method for nondegenerate variational conditions. *Journal of Global Optimization* 28, 405 – 417, 2004
23. Rubin, S., I. Alderman, D. Parter, and M. K. Vernon, Foundations for Intrusion Prevention, *Practice of Information Technology and Communication,* Volume 27, No. 4, October - December 2004. (One of eight "best and most interesting DIMVA 2004 papers" invited for extension and publication.)
24. N. Singpurwalla, Knowledge Management and Information Superiority: A Taxonomy. *Journal of Statistical Planning and Inference* Vol. 115, No. 2, pp. 361-364, 2003
25. N. Singpurwalla, T. R. Bement, J. M. Booker and S. Keller-McNulty, Testing the Untestable: Reliability in the 21st Century, *IEEE Transactions in Reliability* Vol. 52, No. 1, pp. 118-124, 2003
26. N. Singpurwalla and J. Booker, Membership functions and probability measures of fuzzy Sets, *Journal of the American Statistical Association,* vol.99, no.467, p. 867-877, 2004 (with discussion by Dempster, Laviolette, Lindley, and Zadeh)
27. N. Singpurwalla and C. Kong, Specifying interdependence in networked systems, *IEEE Transactions on Reliability,* vol.52, no. 3, p. 401-405, 2004
28. N. Singpurwalla and P. Wilson, When can finite testing ensure infinite trustworthiness?, *J. Iranian Statistical Soc.* Vol. 3, no.1, p.1-37, 2004, (with discussion by Bernardo, Boland, Cox, Higdon, and Nakhleh).
29. N. Singpurwalla, S. McNulty and C. Nakhleh, A Paradigm for Masking (Camouflaging) *Information. International Statistical Review* Vol. 73, pp. 331-349, 2005
30. Schwartz, D.G, Agent-oriented epistemic reasoning: subjective conditions of knowledge and belief, *Artificial Intelligence* 148 177-195 2003
31. S. Stoecklin and C. Allen, Creating a Reusable GUI Component, *Software Practice and Experience* 32, 403-416, 2002
32. B. Zhou, M. Bassiouni and G. Li, Routing and Wavelength Assignment in Optical Networks Using Logical Link Representation and Efficient Bitwise Computation, *Journal of Photonic Network Communications,* Springer Publishing, Vol. 10, No. 3, pp. 333-346, Nov. 2005

33. B. Zhou and M. Bassiouni, Supporting Differentiated Quality of Service in Optical Burst Switched Networks, *SPIE Journal of Optical Engineering*, Vol. 45, 2006

Papers published in non-peer-reviewed journals or in conference proceedings

34. K. Anna, A. Karnik, R. Guha, and M. Chatterjee, Enhancing QoS in 802.11e with Beacon Management, Proceedings of the 7th IEEE International Conference on High Speed Networks and Multimedia Communications, (HSNMC'04), June 30 – July 2, 2004
35. M. Bassiouni, W. Cui and B. Zhou Fast Routing and Recovery Protocols in Hybrid Ad-hoc Cellular Networks, Book Chapter in *Wireless Communications Systems and Networks*, edited by M. Guizani, Kluwer Publishing, pp. 685-697, June 2004
36. M. Bassiouni and R. Guha, Modeling and Analysis of Temporal Failure and Degradation Behavior of Critical Infrastructure Systems, *Proceedings of the 35th Hawaii International Conference on System Sciences*, January 2002
37. J. Bethencourt, J. Franklin, and M. Vernon, Mapping Internet Sensors with Probe Response Attacks, Proc. 14th USENIX Security Symposium, Baltimore, August 2005
38. Bier, V. M., and V. Abhichandani, Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries, *Risk-Based Decisionmaking in Water Resources X*, pp. 59-76, Santa Barbara, California, November 3-8, 2002
39. V. M. Bier, S. Ferson, Y. Y. Haimes, J. H. Lambert, and M. J. Small, Risk of Extreme and Rare Events: Lessons from a Selection of Approaches, in: T. McDaniels and M. J. Small (editors), *Risk Analysis and Society: Interdisciplinary Perspectives*, Cambridge University Press, Cambridge, England, 2003
40. Bier, V. M., plenary speaker, Should the Model for Security Be Game Theory Rather than Reliability Theory?, *Communications of the Fourth International Conference on Mathematical Methods in Reliability: Methodology and Practice*, Santa Fe, New Mexico, June 21-25, 2004 http://www.stat.lanl.gov/MMR2004/Extended%20Abstracts/VBier.pdf
41. Bier, V. M., Game-Theoretic Approaches to Critical Infrastructure Protection, Conference on Reducing the Risks and Consequences of Terrorism, University of Southern California, November 2004 http://www.usc.edu/dept/create/November18/Bier,%20Vicki.ppt
42. Bier, V. M., E. Gratz, N. Haphuriwat, W. Magua, and K. Wierzbicki, Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System, Workshop on Safeguarding National Infrastructures: Integrated Approaches to Failure in Complex Networks, http://www.dcs.gla.ac.uk/~johnson/infrastructure/papers/Vicki.pdf, University of Glasgow, August 25-27, 2005
43. Bier, V. M., Game-Theoretic and Reliability Methods in Counter-Terrorism and Security. *Mathematical and Statistical Methods in Reliability* (A. Wilson, N. Limnios, S. Keller-McNulty, and Y. Armijo, editors), Series on Quality, Reliability and Engineering Statistics, World Scientific, Singapore, 2005, pp. 17-28.

44. Bier, V. M., Hurricane Katrina as a Bureaucratic Nightmare. *On Risk and Disaster: Lessons from Hurricane Katrina* (R. J. Daniels, D. F. Kettl, and H. Kunreuther, editors), University of Pennsylvania Press, Philadelphia, 2006, pp. 243-254.
45. Bier, V. M., Risk Analysis (Homeland Security). *McGraw-Hill Yearbook of Science and Technology 2006*, McGraw-Hill, New York, 2006, pp. 283-284.
46. P. Carayon and S. Kraemer, Macroergonomics in WWDU: What about computer and information system security?, In *Proceedings of the 6th International Scientific Conference on Work With Display Units – WWDU 2002 – World Wide Work,* edited by H. Luczak, A.E. Cakir and G. Cakir, ERGONOMIC Institut fur Arbeits- und Sozialforschung Forschungsgesellschaft mbH, Berlin, Germany, 2002, pp.87-89.
47. P. Carayon, R. Duggan, and S. Kraemer, A model of red team performance. In H. Luczak and K. J. Zink (Eds.), *Human Factors in Organizational Design And Management – VII*, IEA Press, Aachen, Germany, 2003, pp.443-447
48. P. Carayon and S. Kraemer, Using accident analysis methods in computer security: The development of the Human Factors Vulnerability Analysis (HFVA). In *Proceedings of the XVth Triennial Congress of the International Ergonomics Association and the 7th Joint Conference of Ergonomics Society of Korea/Japan Ergonomics Society*, Seoul, Korea, 2003.
49. P. Carayon, S. Kraemer, and V. Bier, Human Factors Issues in Computer and E-Business Security. *Handbook of Integrated Risk Management for E-Business: Measuring, Modeling and Managing Risk* (A. Labbi, editor), J. Ross Publishing, 2005, pp.63-85.
50. J. Chandra, Distributed and decentralized information processing, *Proc. IconIT 2001*, pp.1-11, 2001
51. J. Chandra, S. Guo and L. Shieh, Adaptive control for nonlinear stochastic hybrid systems with input saturation, Proc. 34th HICSS, 2001
52. W. Cui and M. Bassiouni Channel Planning and Fault Recovery in Hierarchical Hybrid Cellular Networks with Mobile Routers, *Proc. IEEE Wireless Local Networks- 26th LCN Conf.*, Nov. 2001, pp. 646-652
53. W. Cui and M. Bassiouni, Adaptive Recovery Protocols for Multi-layer Ad-Hoc Networks in Theater of Non-uniform Failure Rate, *Proceedings of the 16th AeroSense SPIE Conference on Digital Wireless Communications*, pp. 142-150, April 2002
54. Z. Furqan, R. Guha, and S. Muhammad, A Heuristic State Space Search Model for Security Protocol Verification, Proceedings of the First International Conference on E-business and Telecommunication Networks, (ICETE-2004), pp 113 – 118, August 24 – 28, 2004
55. Z. Furqan, S. Muhammad, and R. Guha, Priority Based Channel Assignment with Pair-wise Listen and Sleep Scheduling for Wireless Sensor Networks, Proceedings of the IEEE 8th International Multitopic Conference, pp 522 – 527, December 24 – 26, 2004
56. Z. Furqan, S. Muhammad, R. Guha, Formal Verification of 802.11i using Strand Space Formalism, Proceedings of 5th International Conference on Networking (ICN), IEEE Computer Society Press, Mauritius, April 23 – 28, 2006

57. J. Granger, A. Krishnamurthy, and S. M. Robinson, Stochastic modeling of airlift operations. In: B. A. Peters, J. S. Smith, D. J. Medeiros, and M. W. Rohrer, editors, *Proceedings of the 2001 Winter Simulation Conference,* pp. 432-440
58. J. Granger, A. Krishnamurthy, and S. M. Robinson, Approximation and optimization for stochastic networks. In: K. Marti, Y. Ermoliev, and G. Pflug, eds., *Dynamic Stochastic Optimization,* pp. 67–79. Springer-Verlag (Lecture Notes in Economics and Mathematical Systems No. 532), Berlin 2004
59. R. Guha, O. Kachirski, D. G. Schwartz, S. Stoecklin, and E. Yilmaz, Case-based agents for packet-level intrusion detection in ad hoc networks, *Proceedings of Seventeenth International Symposium on Computer and Information Sciences,* Orlando, FL, pp. 315 – 320, October 28-30, 2002, CRC Press
60. R. Guha, S. Muhammad, and Z. Furqan, A Dynamic Simulation Model and Testing Techniques for Security Protocol Verification, Proceedings of the 4th WSEAS International Conference on Information Science, Communications And Applications (ISA 2004), April 2004
61. R. Guha and O. Kachirski, Load Balancing Approach for the Ad Hoc Wireless Intrusion Detection Simulation Framework, Proceedings of World Wireless Congress, May, 2004
62. R. Guha, K. Anna, A Karnik, and M. Chatterjee, Enhancing QoS in 802.11e with Beacon Management, in Proceedings of the 7th IEEE International Conference on High Speed Networks and Multimedia Communications, Lecture Notes in Computer Science, (Editors: Z. Mammeri, P. Lorenz), Vol. 3079, pp 598-608, Springer, June- July, 2004
63. R. Guha and O. Kachirski, An Architecture For Distributed Simulation Of Wireless Networks, Proceedings of 18th European Simulation Multiconference, pp 34 – 39, June 12 -16, 2004
64. R. Guha, S. Muhammad, and Z. Furqan, A Dynamic Simulation Model and Testing Techniques for Security Protocol Verification, *WSEAS Transaction on Computers*, Volume 3, Issue 5, pp 1226 – 1231, Nov. 2004
65. R. Guha and S. Rakshit, Medium Access and Fair Bandwidth Sharing in WLAN, Proceedings of the IASTED International Conference on Advances In Computer Science And Technology, November 22 – 24, 2004
66. R. Guha and S. Rakshit, Selfish Users and Distributed MAC protocols in Wireless Local Area Networks (WLANs), Proceedings of the Asia Pacific Industrial Engineering and Management Systems Conference 2004, December 12 – 15, 2004
67. R. Guha, S. Muhammad, and Z. Furqan, Wireless Sensor Network Security: A Secure Sink Node Architecture, Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference (IPCCC - IWSEEASN 2005), pp 371 – 376, April 7 – 9, 2005
68. R. Guha, M. Chatterjee and J. Sarkar, A Distributed Security Architecture for Ad hoc Networks, Proceedings of the Fourth International Workshop on Wireless Information Systems, H. Weghorn and Q. Mahmoud (Eds.), pp 81 – 91, May 24 – 25, 2005
69. R. Guha and O. Kachirski, Load Balancing Approach for the Ad Hoc Wireless Intrusion Detection Simulation Framework, Proceedings of World Wireless Congress, May 25 -28, 2004

70. R. Guha, O. Kachirski, D. Schwartz, S. Stoecklin, and Y. Yilmaz, Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks, Proceedings of the 17th International Symposium on Computer and Information Sciences, pp 315 – 320, October 2002, CRC Press
71. R. Guha, J. Lee and O. Kachirski, Evaluating Performance Of Distributed Computing Technologies – HLA And Tspaces, Proceedings of the 19th European Conference on Modeling and Simulation, Y. Merkuryev, R. Zobel, and E. Kerckhoffs (Eds), pp 820- 825, June 1- 4, 2005
72. R. Guha, and D. Purandare, Enhancing Message Privacy in WEP, Proceedings of the Fourth International Workshop on Wireless Information Systems, H. Weghorn and Q. Mahmoud (Eds.), pp 22 – 32, May 24 – 25, 2005
73. R. Guha and S. Rakshit, Selfish Users and Distributed MAC protocols in Wireless Local Area Networks (WLANs), Proceedings of the Asia Pacific Industrial Engineering and Management Systems Conference 2004, December 12 – 15, 2004
74. R. Guha and J. Wang, Improving Web Access Efficiency Using P2P Proxies, Proceedings of 4th International Workshop on Distributed Computing", *Lecture Notes in Computer Science* Vol 2571, Eds: S. Das, S. Bhattacharya, pp 24-34, 2002, Springer Verlag
75. P. Gupta and R. Guha, A Heuristic for Efficient Data Distribution Management in Distributed Simulation, Proceedings of the SPIE Defense and Security Symposium 2005, March 28 – April 1, 2005
76. P. Gupta and R. Guha, Design and Implementation of an Efficient Algorithm for Data Distribution Management in High Level Architecture, Proceedings of 4th Symposium on Design, Analysis, and Simulation of Distributed Systems, 2006 Spring Simulation Multiconference, Huntsville, Alabama, April 2-6, 2006 (CD-ROM)
77. Somesh Jha, Louis Kruger, Thomas G. Kurtz, Yoonjung Lee, Adam Smith, and Zhengxiao Wu, Optimal filtering techniques for intrusion detection, SPIE Proceedings: Defense and Security 2005: Sensory Data Exploitation, Target Recognition, and Information Fusion, Data Mining, and Information Networks Security Technologies
78. O. Kachirski and R. Guha, Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks, *Proceedings of IEEE Knowledge Media Networking Conference*, July 2002
79. O. Kachirski and R. Guha, Effective intrusion detection using multiple sensors in wireless ad hoc networks. *Proceedings of 36th Hawaii International Conference on System Science*, January 2003 (in CD-ROM)
80. K. Karnik, K. Anna, R. Guha, and M. Chatterjee, A smart polling scheme for the 802.11e wireless LANs. In *Proceedings of Huntsville Simulation Conference*, October 29 -31, 2003, (in CD-ROM)
81. A. Kejriwal, R. Guha and M. Chatterjee, User Class based QoS Differentiation in 802.11e WLAN, Proceedings of 18th European Simulation Multiconference, pp 203 - 209, June 12 -16, 2004
82. S. Kraemer and P. Carayon, A human factors vulnerability evaluation method for computer and information security. In *Proceedings of the Human Factors and*

Ergonomics Society, pp. 1389-1393, The Human Factors and Ergonomics Society, Denver, CO, 2003

83. S. Kraemer & P. Carayon (2005). A macroergonomic framework for computer and information security. In P. Carayon, M. Robertson, B. Kleiner & P. Hoonakker (Eds.), *Human Factors in Organizational Design and Management – VII* (pp. 243-254). Santa Monica, CA: IEA Press
84. Kraemer, S., Carayon, P., & Duggan, R. (2004). Red team performance for improved computer and information security. In The Human Factors and Ergonomics Society (Ed.), *Proceedings of the Human Factors and Ergonomics Society* (pp. 1605-1609). New Orleans, LA
85. S. Kraemer & P. Carayon (2005). Computer and information security culture: Findings from two studies. In *Proceedings of the 49th Annual Meeting of the Human Factors and Ergonomics Society*. Orlando, FL: Human Factors and Ergonomics Society, pp. 1483-1487
86. Kraemer, S., Carayon, C., & Clem, J. F. (2006). Characterizing violations in computer and information security systems. In *Proceedings of the 16th Triennial Congress of the International Ergonomics Association*. Maastricht, the Netherlands.
87. Somesh Jha, Louis Kruger, Thomas G. Kurtz, Yoonjung Lee, Adam Smith, and Zhengxiao Wu, Optimal filtering techniques for intrusion detection, SPIE Proceedings: Defense and Security 2005: Sensory Data Exploitation, Target Recognition, and Information Fusion, Data Mining, and Information Networks Security Technologies.
88. J. Lee, H. Zhang, and R. Guha, Virtual Cluster Computing Architecture, Proceedings of the 2005 International Conference on Parallel and Distributive Processing Techniques and Applications, June 27 – 30, 2005.
89. J. Lee, H. Zhang, and R. Guha, Portable and Scalable Parallel Applications with VCluster, Proceedings of the 19th European Conference on Modeling and Simulation, Y. Merkuryev, R. Zobel, and E. Kerckhoffs (Eds), pp 808- 813, June 1-4, 2005.
90. J. Long, S. Stoecklin, D.G. Schwartz, and M. Patel, Adaptive similarity measures in case-based reasoning, The 6th IASTED International Conference on Intelligent Systems and Control (ISC'04), August 23-25, 2004, Honolulu, Hawaii, pp. 260--265.
91. J. Long, D.G. Schwartz, S. Stoecklin, and M. Patel, Application of loop reduction to learning program behaviors for anomaly detection, International Conference on Information Technology: Coding and Computing (ITCC'05), Las Vegas, NV, April 11-13, 2005, pp. 691-696.
92. J. Long, D. Schwartz, and S. Stoecklin, An XML distance measure, The 2005 International Conference on Data Mining, DMIN'05, Las Vegas, Nevada, June 20-23, 2005, pp. 119-125.
93. Long, J., Schwartz, D.G., and Stoecklin, S., Application of case-based reasoning to multi-sensor network intrusion detection, WSEAS/IASME International Conference on Computational Intelligence, Man-Machine Systems, and Cybernetics (CIMMACS'05), Miami, Florida, USA, November 17--19, 2005, pp. 260-269.

94. S. Muhammad, R. Guha, and Z. Furqan, A dynamic simulation model and testing techniques for security protocol verification. Proceedings of the 4th WSEAS International Conference on Information Science, Communications and Applications (ISA 2004), April 2004.
95. S. Muhammad, Z. Furqan, R. Guha, Designing Authentication Protocols: Trends and Issues, Proceedings of 5th International Conference on Networking (ICN), IEEE Computer Society Press, Mauritius, April 23 – 28, 2006.
96. S. Muhammad, Z. Furqan, R. Guha, Understanding the Intruder through Attacks on Cryptographic Protocols, Proceedings of 44th ACM Southeast Conference (ACMSE2006), pp 667 – 672, Melbourne, Florida, USA, March 10 -12, 2006.
97. S. Muhammad, Z. Furqan and R. Guha, Wireless Sensor Network Security: A Secure Sink Node Architecture, Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference (IPCCC - IWSEEASN 2005), pp 371 – 376, April 7 – 9, 2005.
98. C. Partridge, P. Barford, D. D. Clark, S. Donelan, V. Paxson, J. Rexford, and M. K. Vernon, The Internet Under Crisis Conditions: Learning from the Impact of September 11, *NRC CSTB Report*, November 2002, ISBN: 0-309-08702-3. Available online at http://www7.nationalacademies.org/cstb/pub_internet911.html
99. Patel, M., Stoecklin, S., Schwartz, D.G., Graphical user interface using a reflective architecture and XML, The 2004 International Conference on Software Engineering Research and Practice (SERP'04), Las Vegas, NV, June 21--24, 2004, pp. 648-651.
100. D. Purandhare and R. Guha, Fast, Efficient and Secure BSS Transitions, Proceedings of the First International Conference on Computers, Communications and Signal Processing, Kuala Lumpur, Malaysia, November 14 -16, 2005.
101. D. Purandare, R. Guha, and J. Lee, An IV Collision Avoidance Algorithm - Strengthening the WEP, Proceedings of the 2005 International Conference on Wireless Networks (ICWN, 05) June 27 – 30, 2005
102. D. Purandare and R. Guha, Enhancing Message Privacy in WEP, Proceedings of the Fourth International Workshop on Wireless Information Systems, pp 23-32, May , 2005
103. S. Rakshit and R. Guha, Optimal Strategies in MAC Protocols, Proceedings of the IEEE International Conference on Communications (ICC-2004), June 21 – 24, 2004.
104. S.M. Robinson, Aspects of the projector on prox-regular sets. In: F. Giannessi and A. Maugeri, eds., *Variational Analysis and Applications*, pp. 963 – 973. Springer SBM, New York 2005.
105. S. Rubin, I. D. Alderman, D.W. Parter, and M. K. Vernon, Foundations for Intrusion Prevention, Proceedings for the Workshop on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2004), Dortmund, Germany, July 2004.
106. D. G. Schwartz, S. Stoecklin, and E. Yilmaz, A Case-Based Approach to Network Intrusion Detection, *Fifth International Conference on Information Fusion, IF'02*, Annapolis, MD, July 7-11, 2002, pp. 1084-1089.
107. N. Singpurwalla, Dependence in Network Reliability, *Proceedings of the 5th International Conference on Information Fusion (2002)*, pp. 981-985.

108. N. Singpurwalla, Stochastic Process Models for Reliability in Dynamic Environments. In C. R. Rao and R. Khattre (Editors), *Handbook of Statistics,* Elsevier Science B.V., The Netherlands, 2003, pp. 1109 – 1129
109. N. Singpurwalla, Warranty a surrogate of reliability. In R. Soyer, T. Mazzuchi, and N. Singpurwalla (Editors), *Mathematical Reliability: An Expository Perspective* (International Series in Operations Research and Management), Kluwer Academic Publishers, Norwell, MA, 2003, pp. 317-333
110. N. Singpurwalla, Predicting damage. In K. Doksum and B. Lindquist (Editors), *Mathematical and Statistical Methods in Reliability,* World Scientific Publishing Company, Singapore, 2003. pp. 267-282
111. Smith, S. and Stoecklin, S., What We Can Learn from Extreme Programming, *The Journal of Computing in Small Colleges, Proceedings of the Fifteenth Annual CCSC Southeastern Conference,* Vol. 17, No. 2, December 2001, pp. 135-142
112. S. Smith, S. Stoecklin, and J. Mullins, Taking Cohesion into the Classroom, Eighteenth Annual Consortium for Computing Sciences in Colleges, Southeastern Conference, at Wofford College in Spartanburg, South Carolina, November 5-6, 2004
113. S. Smith, S. Stoecklin, and J. Mullins, A Practical Guide to Measuring Method Coupling in Object-oriented Systems, IASTED International Conference on Software Engineering and Applications (SEA 2004), MIT Cambridge, November 9-11, 2004.\
114. S. Stoecklin and C. Allen, Creating a Reusable GUI Component, *Software Practice and Experience* 32 (2002) 403-416
115. S. Stoecklin and R. Riggs, Analysis of Automated Code Refactoring, *Eighth International Conference on Information Systems Analysis and Synthesis, SCI2002/ISAS2002,* Orlando, Florida, July 14-18, 2002
116. S. Stoecklin and J. Mullins, Teaching Reflective Architectures, Educational Symposium, *Seventeenth ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications,* Seattle, Washington, November 4-8, 2002
117. Stoecklin, S., Schwartz, D.G., Yilmaz, E., and Patel, M., A metadata architecture for case-based reasoning, The 2004 International Conference on Artificial Intelligence (IC-AI'04), Las Vegas, NV, June 21--24, 2004, pp. 790-794
118. A. Swift, Models for Assessing Network Reliability, *Mathematical Reliability: An Expository Perspective* (Soyer, Mazzuchi and Singpurwalla, Eds), pp. 55-68.(2004)
119. E. Yilmaz, S. Stoecklin, and D. Schwartz, Toward a generic case-based reasoning framework using adaptive software architectures. In *Proceedings of the 2003 International Conference on Information and Knowledge Engineering (IKE'03),* Las Vegas, NV, June 23-26, 2003, Volume II, pp. 512-513 (poster presentation)
120. B. Zhou and M. Bassiouni Geolocation-Based Routing In Wireless Ad-Hoc Networks, in the *Proceedings of the 5th World Wireless Congress,* San Francisco, May 2004
121. Zimmerman, R., and V. M. Bier, Risk Assessment of Extreme Events, Columbia-Wharton/Penn Roundtable on “Risk Management Strategies in an Uncertain World,”

http://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/zimmerman_wp.pdf, Palisades, New York, April 12-13, 2002

Papers presented at meetings, but not published in conference proceedings

122. Bier, V. M., and T. Cox, Game Theoretic Models for Critical Infrastructure Protection. SRA Annual Meeting, Seattle, Washington, December 2-5, 2001
123. Bier, V. M., and V. Abhichandani, Game-theoretic Models for Critical Infrastructure Protection, INFORMS Annual Meeting 2002, San Jose, California, November 17-20, 2002
124. Bordley, R., N. T. Argon, and V. M. Bier, Updating Joint Prior Distributions on Model Inputs and Outputs, with an Application to Simulation, INFORMS Annual Meeting, Atlanta, Georgia, October 19-22, 2003
125. Bier, V. M., Risk Assessment: A Game Theoretic Approach, Ninth U.S. Army Conference on Applied Statistics, Napa Valley, California, October 29-31, 2003
126. Bier, V. M., and S.-W. Lin, A Study of Expert Calibration, Society for Risk Analysis 2003 Annual Meeting, Baltimore, Maryland, December 7-10, 2003
127. Bier, V. M., and A. Nagaraj, Optimal and Near-Optimal Resource Allocations for Critical Infrastructure Protection, SRA 2003 Annual Meeting, Baltimore, Maryland, December 7-10, 2003
128. Bier, V. M., and S.-W. Lin, A Study of Expert Overconfidence, INFORMS Annual Meeting, Denver, October 2004
129. Bier, V. M., Game-Theoretic Methods in Counter-Terrorism and Security, Society for Risk Analysis 2005 Annual Meeting, Orlando, Florida, December 4-7, 2005
130. Bier, V., Game-Theoretic Methods in Counter-Terrorism and Security, Sauk Institute for Leadership, December 2005
131. Bier, V., Game-Theoretic Methods in Counter-Terrorism and Security, American Society for Industrial Security (ASIS), Central Wisconsin Chapter, March 2006
132. Carayon, P., & Kraemer, S. (2005, July 22-25). *Teleworking - The human and organizational issues of computer and information security.* Paper presented at the 11th Annual Conference on Human-Computer Interaction, Las Vegas, NV
133. J. Chandra, Information fusion for critical infrastructure protection. Presented at SMiS Fifth Annual Conference on Military Data Fusion, September, 2003
134. J. Chandra, Overview, problem description, and challenges. Presented at Special Session on Robust Resilient Critical Infrastructure Systems, U.S. Army Conference on Applied Statistics, Napa, CA, October 2003
135. J. Granger, A. Krishnamurthy, and S. M. Robinson, Fast improvement of simulated networks, 2001 U. S. Army Operations Research Symposium, Ft. Lee, VA, October 2001
136. J. Granger, A. Krishnamurthy, and S. M. Robinson, Optimizing performance in networked systems, Presented at Special Session on Robust Resilient Critical Infrastructure Systems, U.S. Army Conference on Applied Statistics, Napa, CA, October 2003
137. Gupta, A., and V. M. Bier, Myopic Agents and Interdependent Security Risks, INFORMS 2004 Meeting, Denver, Colorado, October 24-27, 2004

138. Somesh Jha, Thomas G. Kurtz, and Yoonjung Lee. Application of Filtering Methods to Intrusion Detection, Filtering Theory and Applications 2002, Edmonton, Alberta, July 25 - 30,2002
139. Kraemer, S., and Carayon, P. *Information support systems and computer and information security.* Paper presented at the Intelligent Decision Support Systems: Retrospect and Prospects, Siena, Italy, 2005
140. Thomas G. Kurtz, Somesh Jha, Yoonjung Lee, and Adam Smith. Optimal Filtering Techniques for Intrusion Detection. Presented at Special Session on Robust Resilient Critical Infrastructure Systems, U.S. Army Conference on Applied Statistics, Napa, CA, October 2003
141. Magua, W., Vulnerabilities of Electrical Transmission Systems, InfraGard Superconference, Wisconsin, May 2006
142. S. Oliveros, V. M. Bier, and L. Samuelson, Choosing What to Protect: Strategic Defense Allocation against an Unknown Attacker, INFORMS Annual Meeting 2005, San Francisco, California, November 13-16, 2005
143. N. Singpurwalla, Y. Cui and C. Kong, Information fusion for damage prediction, INFORMS National Meeting, San Jose, CA, Nov. 2002
144. N. Singpurwalla, A mathematical paradigm for sensor fusion. Presented at Special Session on Robust Resilient Critical Infrastructure Systems, U.S. Army Conference on Applied Statistics, Napa, CA, October 2003
145. N. Singpurwalla, Camouflaging Information. Presented at Special Session on Robust Resilient Critical Infrastructure Systems, U.S. Army Conference on Applied Statistics, Napa, CA, October 2003
146. J. Zhuang and V. M. Bier, Subsidized Security and Stability of Equilibrium Solutions in an N-Player Game with Errors, INFORMS Annual Meeting 2005, San Francisco, California, November 13-16, 2005

Manuscripts submitted, but not published

147. Azaiez, N., and V. M. Bier, Optimal Resource Allocation for Security in Reliability Systems, accepted, *European Journal of Operational Research*, 2006
148. M. Bassiouni, V.M. Bier, P. Carayon, J. Chandra, R.K. Guha, S.B. Kraemer, S.M. Robinson, D.G. Schwartz, and S. Stoecklin, Analysis, modeling, and simulation for networked systems, submitted 2004 to volume to be edited by Steven E. King et al., title and publisher unknown
149. Bier, V. M., Choosing What to Protect, accepted, *Risk Analysis*, 2006
150. Bier, V. M., and S.-W. Lin, A Study of Expert Overconfidence, submitted to *Decision Analysis*, 2006
151. Bier, V. M., E. R. Gratz, N. J. Haphuriwat, W. Magua, and K. Wierzbicki, Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System, submitted to *Reliability Engineering and System Safety*, 2005
152. Bier, V. M., and A. Gupta, Myopia and Interdependent Security Risks, submitted to *The Engineering Economist*, 2005
153. Bier, V. M., S. Oliveros, and L. Samuelson, Choosing What to Protect: Strategic Defensive Allocation against an Unknown Attacker, in press, *Journal of Public Economic Theory*, 2006

154. Bier, V. M., Game-Theoretic and Reliability Methods in Counter-Terrorism and Security, in press, *Statistical Methods in Counter-Terrorism* (A. Wilson, G. Wilson, and D. Olwell, editors), Springer, 2006
155. P. Carayon, Human factors of complex sociotechnical systems, *Applied Ergonomics*, 2006 (to appear)
156. Z. Furqan, S. Muhammad, R. Guha, Authentication Analysis of 802.11i Protocol, Submitted to *Journal of Computers and Security*, 2005
157. R. Guha and D. Purandare, Security Issues in BitTorrent like P2P Streaming Systems to appear in the Proceedings of Summer Computer Simulation Conference, Calgary, Canada, July 31-August 2, 2006
158. P. Gupta and R. Guha, Design, Analysis, and Performance Evaluation of an Efficient Algorithm for Data Distribution Management in High Level Architecture, revised and resubmitted to the *Journal of Defense Modeling and Simulation*, 2006
159. P. Gupta and R. Guha, Data Distribution Management for High Performance Distributed Simulation in Resource-Constraint Environment, to appear in the Proceedings of the 20th European Simulation Multiconference, Bonn, Germany, May 28-31, 2006
160. P. Gupta and R. Guha, Integration of the P-Pruning Data Distribution Management Technique with FDK, to appear in the Proceedings of Summer Computer Simulation Conference, Calgary, Canada, July 31-August 2, 2006
161. P. Gupta and R. Guha, A Multi-Dimensional Dynamic Data Distribution Management Technique for Distributed Simulation, 2006 Fall SIW, Orlando, Sept. 10-15, 2006 (submitted)
162. Kraemer, S., and Carayon, P. Human and organizational factors in the computer and information security of interoperable systems. To be published in: P. C. Cacciabue, E. Hollnagel, D. D. Woods, J. Wilson, A. Rizzo & P. Sanderson (Eds.), *Intelligent Decisions? Intelligent Support?* (2006)
163. Kraemer, S.B. and Carayon, P. Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists, *Applied Ergonomics*, 2006 (to appear)
164. Kraemer, S., and Carayon, P. Security managers' views of human and organizational factors and computer and information security. Resubmitted to *Computers & Security* in January 2006
165. Kraemer, S., Carayon, P., and Clem, J. Red teams in computer and information security: An assessment of performance. Resubmitted to *Human Factors* in November 2005
166. Thomas G. Kurtz and Shun-Hwa Li. Time invariance modeling and estimation for spatial point processes: General theory. Under revision for *Bernoulli*
167. Nancy Lopes Garcia and Thomas G. Kurtz. Spatial birth and death processes as solutions of stochastic equations. *ALEA* (to appear, 2006)
168. Long, J., Schwartz, D., and Stoecklin, S., Case-oriented alert correlation, *Journal of Computer Security*, submitted 3/2006, in review
169. Long, J., Schwartz, D., and Stoecklin, S., Improving the effectiveness of Snort by clustering patterns of alerts, *ACM Transactions on Information and Systems Security*, submitted 3/2006, in review

170. S. Lu and S.M. Robinson, Variational inequalities over perturbed polyhedral convex sets. Submitted 2006 to *Mathematics of Operations Research*
171. D. Purandare and R. Guha, Preferential and Strata based P2P Model: Selfishness to Altruism and Fairness, to appear in the Proceedings of International Conference on Parallel and Distributed Systems," July 12 -15, 2006
172. D. Purandare and R. Guha, BEAM: An Efficient Peer to Peer Media Streaming Framework, The 31st IEEE Conference on Local Area Networks, November 14 -17, 2006, Tampa, Florida, (submitted)
173. S.M. Robinson, Strong regularity and the sensitivity analysis of transportation equilibria: A comment. *Transportation Science*, in press.
174. S.M. Robinson, Calmness and Lipschitz continuity for multifunctions. Submitted 2006 to *SIAM Journal on Optimization*
175. A. Swift, Models for cascading failures, *J. Applied Probability* (to appear)
176. Zhuang, J., and V. M. Bier, Subsidized Security and Stability of Equilibrium Solutions in an N-Player Game with Errors, submitted to *Games and Economic Behavior*, 2006
177. Zhuang, J., and V. M. Bier, Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort, submitted to *Operations Research*, 2006

Technical reports submitted to ARO

None

List of all participating scientific personnel

(showing any advanced degrees earned by them while employed on the project)

Certain participating personnel received the Ph.D. with a degree date subsequent to the April 2006 termination of the period of performance. Those personnel are listed below with the notation "Ph.D. 2006."

Vinod Abhichandani, Research Assistant (MSIE)
Ian Alderman, Research Assistant
Sommer Alexander, Undergraduate (BSIE)
Kiran Anna, Research Assistant
Mostafa Bassiouni, Professor
John Bethencourt, Undergraduate (BS)
Vicki M. Bier, Professor
Pascale Carayon, Professor
Jagdish Chandra, Research Professor
Wei Cui 1[1], Research Assistant (Ph.D.)
Wei Cui 2 [1], Research Assistant
Nikhil Dighe, Research Assistant

[1] Two students at the University of Central Florida, both named Wei Cui, participated in the work of this grant. They are listed here as Wei Cui 1 and Wei Cui 2.

Mounire ElHoumaidi (Not supported but worked on publications acknowledging this grant) (Ph.D.)
Ya-Ju Fan, Research Assistant
Jason Franklin, Undergraduate (BS)
Zeeshan Furquan, Research Assistant (MS)
Julien Granger, Research Assistant (Ph.D. 2006)
Eli Gratz (Not supported but worked on publications acknowledging this grant)
Ratan Guha, Professor
Ashish Gupta, Research Assistant (MSIE)
Pankaj Gupta, Research Assistant (MS)
Naraphorn Haphuriwat, Research Assistant
Oleg Kachirski, Research Assistant (Ph.D.)
Abhishek Karnik, Research Assistant
Amit Kejriwal, Research Assistant
Sara Kraemer, Research Assistant (MSIE, Ph.D. 2006)
Louis Kruger, Research Assistant
Thomas G. Kurtz, Professor
Josh Landon, Research Assistant
Yoonjung Lee, Research Assistant (Ph.D.)
Marco Lemp, Research Assistant, (MS)
Shi-Woei Lin, Research Assistant (Ph.D.)
Wayne Liu, Research Assistant
Jidong Long, Research Assistant (Ph.D. 2006)
Shu Lu, Research Assistant (MSIE 2006)
Wairimu Magua (Not supported but worked on publications acknowledging this grant)
Sahabuddin Muhammad, Research Assistant (MS)
Aniruddha Nagaraj, Research Assistant (MSIE)
Niyazi Oztoprak, Undergraduate (BSIE)
David Parter, Research Associate
Mahesh Patel, Research Assistant (MS)
Darshan Purandare, Research Assistant (MS)
Sudipta Rakshit, Research Assistant (Ph.D.)
Stephen M. Robinson, Professor
Shai Rubin, Research Assistant
Daniel Schwartz, Associate Professor
Adam Secada, Undergraduate
Nozer Singpurwalla, Professor
Adam Smith, Research Assistant
Sara Stoecklin, Associate-In Computer Science
Andrew Swift, Research Assistant
Yi-Chun Tsai, Research Assistant
Mary K. Vernon, Professor
Kevin Wierzbicki (Not supported but worked on publications acknowledging this grant) (MS)
Philip Wilson, Research Assistant
Zhengxiao Wu, Research Assistant

Miaomiao Xu, Research Assistant (MS)
Erbil Yilmaz, Research Assistant
Hua Zhang, Research Assistant
Bin Zhou, Research Assistant (Ph.D.2006)

Report of Inventions (by title only)

None

Bibliography

All bibliographic items appear in the foregoing list of publications.

Appendices

None