# REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188



| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (From - To) |
|---|---|---|
| 19-04-2022 | Final Report | 24-Jun-2013 - 23-Jun-2019 |

**4. TITLE AND SUBTITLE**
Final Report: 5.3 Information and Software Assurance: Resiliency, Security, and Trust in Complex Engineered Systems

**5a. CONTRACT NUMBER**
W911NF-13-1-0086

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHORS**

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAMES AND ADDRESSES**
University of Illinois - Urbana - Champaign
c/o Office of Sponsored Programs
1901 S. First Street, Suite A
Champaign, IL 61820 -7406

**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. SPONSOR/MONITOR'S ACRONYM(S)**
ARO

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
63047-NS.67

**12. DISTRIBUTION AVAILIBILITY STATEMENT**
Approved for public release; distribution is unlimited.

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

**14. ABSTRACT**

**15. SUBJECT TERMS**

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 15. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | David Nicol |
| UU | UU | UU | UU | | 19b. TELEPHONE NUMBER 217-244-1925 |

# RPPR Final Report
as of 09-Aug-2022

Agency Code: 21XD

Proposal Number: 63047NS **Agreement Number: W911NF-13-1-0086**
**INVESTIGATOR(S):**

**Name:** David M. Nicol
**Email:** dmnicol@illinois.edu
**Phone Number:** 2172441925
**Principal:** Y

Organization: **University of Illinois - Urbana - Champaign (UIUC)**
Address: c/o Office of Sponsored Programs, Champaign, IL 618207406
Country: USA
DUNS Number: 041544081 EIN: 376000511
**Report Date:** 23-Sep-2019 Date Received: 19-Apr-2022
**Final Report** for Period Beginning 24-Jun-2013 and Ending 23-Jun-2019
**Title:** 5.3 Information and Software Assurance: Resiliency, Security, and Trust in Complex Engineered Systems
**Begin Performance Period:** 24-Jun-2013 **End Performance Period:** 23-Jun-2019
**Report Term:** 0-Other
Submitted By: Andrea Whitesell Email: whitesel@illinois.edu
Phone: (217) 333-2399


**STEM Degrees:** **STEM Participants:**

**Major Goals:** The University of Illinois at Urbana-Champaign proposes to perform research in the resiliency, security, and trustworthiness of complex systems involving computers, communications, control, and humans, with application to specific topics of interest to ARO. The research will leverage the significant personnel and resources assembled through the Information Trust Institute (ITI), to perform ground-breaking research in the design of trust-worthy complex systems, with an emphasis on the quantitative assessment of the resiliency, security, and trust properties of those systems. The design elements include system architectures, software, hardware, and algorithms; the designs rest upon models and principles from which provable and quantifiable properties can be derived, using mathematical models and methodologies based on techniques drawn from control theory, stochastic systems, decision and game theory, and formal methods. Assessment work also includes development of prototypical software tools for design and decision support. Comprised of over 90 faculty and a dozen technical staff, ITI researchers aim to place the study of security, resiliency, and trust on a firm scientific and engineering basis. The projects ITI takes on span the application space, including control of cyber-physical systems, health information security and privacy, cloud computing, avionics, communication, and computing. ITI is a capable organization for solving foundational and critical DoD problems in trustworthy systems space.

**Accomplishments:** A PDF outlining the accomplished goals is attached.

**Training Opportunities:** Nothing to Report

**Results Dissemination:** A PDF outlining results dissemination is attached.

**Honors and Awards:** Nothing to Report

**Protocol Activity Status:**

**Technology Transfer:** Nothing to Report

**PARTICIPANTS:**

**Participant Type:** Faculty
**Participant:** Ravi Iyer
**Person Months Worked:** 15.00 **Funding Support:**

Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Sayan Mitra
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Adam Slagell
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Catello DiMarino
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Geir Dullerud
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** M. Tamer Basar
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Quanyan Zhu
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Gul Agha
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

# RPPR Final Report
as of 09-Aug-2022

**Participant Type:** Graduate Student (research assistant)
**Participant:** Kirill Mechitov
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Peter Dinges
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** PD/PI
**Participant:** David Nicol
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Mouna Bamba
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Jose Meseguer
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Santigo Escobar
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Co PD/PI
**Participant:** William Sanders
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

# RPPR Final Report
as of 09-Aug-2022

**Participant Type:** Graduate Student (research assistant)
**Participant:** Michael Ford
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Ken Keefe
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Nikita Borisov
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Naresh Shanbhag
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Joseph Sloan
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Tim Bretl
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Navid Aghasadeghi
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty

**Participant:** Shobha Vasudevan
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Parth Sagdeo
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Chen-Hsuan Lin
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Brighten Godfrey
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Ahmed Khursid
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Wenxuan Zhu
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Yuguo Chen
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Jenny Applequist
**Person Months Worked:** 15.00 **Funding Support:**

Project Contribution:
National Academy Member: N

**Participant Type:** Staff Scientist (doctoral level)
**Participant:** Zbigniew Kalbarczyk
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Elsa Gunter
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Rakesh Kumar
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Staff Scientist (doctoral level)
**Participant:** Rakesh Kumar
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Staff Scientist (doctoral level)
**Participant:** Sibin Mohan
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Staff Scientist (doctoral level)
**Participant:** Rayaduram Srikant
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Sean Smith
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Ross Koppel
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Jim Blythe
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Faculty
**Participant:** Grace Gao
**Person Months Worked:** 15.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Other Professional
**Participant:** Brett Federsen
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Atul Bohara
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Carmen Cheh
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Ahmed Fawaz
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

# RPPR Final Report
as of 09-Aug-2022

**Participant Type:** Graduate Student (research assistant)
**Participant:** Mohamed Noureddine
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Uttam Thakore
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Benjamin Ujcich
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Ashwin Kanhere
**Person Months Worked:** 13.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**Participant Type:** Graduate Student (research assistant)
**Participant:** Arthur Chu
**Person Months Worked:** 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

**ARTICLES:**

# RPPR Final Report
as of 09-Aug-2022

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** FOCLASA 2012
Publication Identifier Type: DOI Publication Identifier: 10.4204/EPTCS.91.2
Volume: 91 Issue: 0 First Page #: 16
Date Submitted: Date Published:
Publication Location:
**Article Title:** Parameterized Concurrent Multi-Party Session Types
**Authors:**
**Keywords:** PROGRAMMING LANGUAGES, DISTRIBUTED, PARALLEL, CLUSTER COMPUTING
**Abstract:** Session types have been proposed as a means of statically verifying implementations of communication protocols. Although prior work has been successful in verifying some classes of protocols, it does not cope well with parameterized, multi-actor scenarios with inherent asynchrony. For example, the sliding window protocol is inexpressible in previously proposed session type systems. This paper describes System-A, a new typing language which overcomes many of the expressiveness limitations of prior work. System-A explicitly supports asynchrony and parallelism, as well as multiple forms of parameterization. We define System-A and show how it can be used for the static verification of a large class of asynchronous communication protocols.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** ACM Computing Surveys
Publication Identifier Type: DOI Publication Identifier: 10.1145/2480741.2480742
Volume: 45 Issue: 3 First Page #: 1
Date Submitted: Date Published:
Publication Location:
**Article Title:** Game theory meets network security and privacy
**Authors:**
**Keywords:** computer systems organization, security and privacy, network security
**Abstract:** This survey provides a structured and comprehensive overview of research on security and privacy in computer and communication networks that use game-theoretic approaches. We present a selected set of works to highlight the application of game theory in addressing different forms of security and privacy problems in computer networks and mobile applications. We organize the presented works in six main categories: security of the physical and MAC layers, security of self-organizing networks, intrusion detection systems, anonymity and privacy, economics of network security, and cryptography. In each category, we identify security problems, players, and game models. We summarize the main results of selected works, such as equilibrium analysis and security mechanism designs. In addition, we provide a discussion on the advantages, drawbacks, and future direction of using game theory in this field. In this survey, our goal is to instill in the reader an enhanced understanding of different res
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

# RPPR Final Report
as of 09-Aug-2022

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** The International Journal of Robotics Research
Publication Identifier Type: DOI Publication Identifier: 10.1177/0278364912473169
Volume: 33 Issue: 1 First Page #: 0
Date Submitted: Date Published:
Publication Location:
**Article Title:** Quasi-static manipulation of a Kirchhoff elastic rod based on a geometric analysis of equilibrium configurations
**Authors:**
**Keywords:** static equilibrium,
**Abstract:** Consider a thin, flexible wire of fixed length that is held at each end by a robotic gripper. Any curve traced by this wire when in static equilibrium is a local solution to a geometric optimal control problem, with boundary conditions that vary with the position and orientation of each gripper. We prove that the set of all local solutions to this problem over all possible boundary conditions is a smooth manifold of finite dimension that can be parameterized by a single chart. We show that this chart makes it easy to implement a sampling-based algorithm for quasi-static manipulation planning. We characterize the performance of such an algorithm with experiments in simulation.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** IEEE Transactions on Robotics
Publication Identifier Type: DOI Publication Identifier: 10.1109/TRO.2012.2218911
Volume: 29 Issue: 1 First Page #: 0
Date Submitted: Date Published:
Publication Location:
**Article Title:** Mechanics and Quasi-Static Manipulation of Planar Elastic Kinematic Chains
**Authors:**
**Keywords:** chains, discrete time systems, elasticity, manipulator kinematics, optimal control
**Abstract:** In this paper, we study quasi-static manipulation of a planar kinematic chain with a fixed base in which each joint is a linearly elastic torsional spring. The shape of this chain when in static equilibrium can be represented as the solution to a discrete-time optimal control problem, with boundary conditions that vary with the position and orientation of the last link. We prove that the set of all solutions to this problem is a smooth three-manifold that can be parameterized by a single chart. Empirical results in simulation show that straight-line paths in this chart are uniformly more likely to be feasible (as a function of distance) than straight-line paths in the space of boundary conditions. These results, which are consistent with an analysis of visibility properties, suggest that the chart we derive is a better choice of space in which to apply a sampling-based algorithm for manipulation planning. We describe such an algorithm and show that it is easy to implement.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** IEEE Security & Privacy
Publication Identifier Type: DOI Publication Identifier: 10.1109/MSP.2013.110
Volume: 11 Issue: 5 First Page #: 0
Date Submitted: Date Published:
Publication Location:
**Article Title:** Circumvention of Security: Good Users Do Bad Things
**Authors:**
**Keywords:** security of data, security circumvention, usability
**Abstract:** Conventional wisdom is that the textbook view describes reality, and only bad people (not good people trying to get their jobs done) break the rules. And yet it doesn't, and good people circumvent.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

# RPPR Final Report
as of 09-Aug-2022

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** ACM Transactions on Sensor Networks
Publication Identifier Type: DOI Publication Identifier: 10.1145/2489253.2489256
Volume: 9 Issue: 4 First Page #: 0
Date Submitted: Date Published:
Publication Location:
**Article Title:** Performance evaluation of sensor networks by statistical modeling and euclidean model checking
**Authors:**
**Keywords:** wireless sensor network, probability mass function, Euclidean model checking
**Abstract:** Modeling and evaluating the performance of large-scale wireless sensor networks (WSNs) is a challenging problem. The traditional method for representing the global state of a system as a cross product of the states of individual nodes in the system results in a state space whose size is exponential in the number of nodes. We propose an alternative way of representing the global state of a system: namely, as a probability mass function (pmf) which represents the fraction of nodes in different states. A pmf corresponds to a point in a Euclidean space of possible pmf values, and the evolution of the state of a system is represented by trajectories in this Euclidean space. We propose a novel performance evaluation method that examines all pmf trajectories in a dense Euclidean space by exploring only finite relevant portions of the space. We call our method Euclidean model checking. Euclidean model checking is useful both in the design phase—where it can help determine system parameters bas
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** IEEE TRANSACTIONS ON Automatic Control
Publication Identifier Type: Publication Identifier:
Volume: 59 Issue: 9 First Page #: 2340
Date Submitted: Date Published:
Publication Location:
**Article Title:** Control of Linear Switched Systems with Receding Horizon Modal Information
**Authors:**
**Keywords:** Discrete-tim LQG, receding-horizon type control, semidefinite programming
**Abstract:** We address a discrete-time LQG control problem over a fixed performance window and apply a receding-horizon type control strategy, resulting in an exact solution to the problem in terms of semidefinite programming. The systems considered take parameters from a finite set, and switch between them according to an automaton. The controller has a finite preview of future parameters, beyond which only the set of parameters is known. We provide necessary and sufficient convex conditions for the existence of a controller which guarantees both exponential stability and finite-horizon performance levels for the system; the performance levels may differ according to the particular parameter sequence within the performance window. A simple, physics-based example is provided to illustrate the main results.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

# RPPR Final Report
as of 09-Aug-2022

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** American Society for Mechanical Engineers Journal of Dynamic Systems
Publication Identifier Type: Publication Identifier:
Volume: 136 Issue: 3 First Page #: 0
Date Submitted: Date Published:
Publication Location:
**Article Title:** Stabilization of Markovian Jump Linear Systems with Limited Information
**Authors:**
**Keywords:** Markovian jump linear systems
**Abstract:** This paper is concerned with mean-square stabilization of single-input Markovian jump linear systems (MJLSs) with logarithmically quantized state feedback. We introduce the concepts and provide explicit constructions of stabilizing mode-dependent logarithmic quantizers together with associated controllers, and a semi-convex way to determine the optimal (coarsest) stabilizing quantization density. An example application is presented as a special case of the developed framework, that of feedback stabilizing a linear timeinvariant (LTI) system over a log-quantized erasure channel. A hardware implementation of this application on an inverted pendulum testbed is provided using a finite word-length approximation.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** IEEE Security & Privacy
Publication Identifier Type: Publication Identifier:
Volume: 12 Issue: 5 First Page #: 82
Date Submitted: Date Published:
Publication Location:
**Article Title:** Building Reliable and Secure Virtual Machines Using Architectureal Invariants
**Authors:**
**Keywords:** Reliability, Security, Cloud Computing
**Abstract:** Reliability and security tend to be treated separately because they appear orthogonal: reliability focuses on accidental failures, security on intentional attacks. Because of the apparent dissimilarity between the two, tools to detect and recover from different classes of failures and attacks are usually designed and implemented differently. So, integrating support for reliability and security in a single framework is a significant challenge. Here, we discuss how to address this challenge in the context of cloud computing, for which reliability and security are growing concerns. Because cloud deployments usually consist of commodity hardware and software, efficient monitoring is key to achieving resiliency. Although reliability and security monitoring might use different types of analytics, the same sensing infrastructure can provide inputs to monitoring modules.
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

# RPPR Final Report
as of 09-Aug-2022

**Publication Type:** Journal Article Peer Reviewed: N **Publication Status:** 1-Published
**Journal:** IEEE Control System Magazine
Publication Identifier Type: Publication Identifier:
Volume: 35 Issue: 1 First Page #: 46
Date Submitted: Date Published:
Publication Location:
**Article Title:** Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems
**Authors:**
**Keywords:** Roubustness, Security, Cyberphysical Control Systems
**Abstract:** Critical infrastructures, such as power grids and transportation systems, are increasingly using open networks for operation. The use of open networks poses many challenges for control systems. The classical design of control systems takes into account modeling uncertainties as well as physical disturbances, providing a multitude of control design methods such as robust control, adaptive control, and stochastic control. With the growing level of integration of control systems with new information technologies, modern control systems face uncertainties not only from the physical world but also from the cybercomponents of the system. The vulnerabilities of the software deployed in the new control system infrastructure will expose the control system to many potential risks and threats from attackers. Exploitation of these vulnerabilities can lead to severe damage as has been reported in various news outlets [1], [2]. More recently, it has been reported in [3] and [4] that a computer worm,
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**Publication Type:** Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
**Journal:** Automatica
Publication Identifier Type: Publication Identifier:
Volume: 59 Issue: 0 First Page #: 182
Date Submitted: Date Published:
Publication Location:
**Article Title:** Minimax Control over Unreliable Communications Channels
**Authors:**
**Keywords:** Minimax control, unreliable communication channels, zero-sum dynamic games, networked control systems
**Abstract:** In this paper, we consider a minimax control problem for linear time-invariant (LTI) systems over unreliable communication channels. This can be viewed as an extension of the H? optimal control problem, where the transmission from the plant output sensors to the controller, and from the controller to the plant are over sporadically failing channels. We consider two different scenarios for unreliable communication. The first one is where the communication channel provides perfect acknowledgments of successful transmissions of control packets through a clean reverse channel, that is the TCP (Transmission Control Protocol). Under this setting, we obtain a class of output feedback minimax controllers; we identify a set of explicit threshold-type existence conditions in terms of the H? disturbance attenuation parameter and the packet loss rates that guarantee stability and performance of the closed-loop system. The second scenario is one where there is no acknowledgment of successful transm
**Distribution Statement:** 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

**CONFERENCE PAPERS:**

# RPPR Final Report
as of 09-Aug-2022

**Publication Type:** Conference Paper or Presentation **Publication Status:** 1-Published
**Conference Name:** 3rd IEEE Conference on Network Softwarization (NetSoft 2017)
Date Received: 17-Aug-2017 Conference Date: 03-Jul-2017 Date Published: 03-Jul-2017
Conference Location: Bologna, Italy
**Paper Title:** Towards an Accountable Software-Defined Networking Architecture
**Authors:** Benjamin E. Ujcich, Andres Miller, Adam Bates, William H. Sanders
Acknowledged Federal Support: **Y**

**Publication Type:** Conference Paper or Presentation **Publication Status:** 2-Awaiting Publicat
**Conference Name:** 14th International Conference on Quantitative Evaluation of Systems (QEST 2017)
Date Received: 17-Aug-2017 Conference Date: 05-Sep-2017 Date Published: 05-Sep-2017
Conference Location: Berlin, Germany
**Paper Title:** Data-Driven Model-Based Detection of Malicious Insiders via Physical Access Logs
**Authors:** C. Cheh, B. Chen, W.G. Temple, W.H. Sanders
Acknowledged Federal Support: **Y**

**Publication Type:** Conference Paper or Presentation **Publication Status:** 0-Other
**Conference Name:** 36th IEEE International Symposium on Reliable Distributed Systems (SRDS 2017)
Date Received: 17-Aug-2017 Conference Date: 26-Sep-2017 Date Published: 26-Sep-2017
Conference Location: Hong Kong, China
**Paper Title:** An Unsupervised Multi-Detector Approach for Identifying Malicious Lateral Movement
**Authors:** Atul Bohara, Mohammad A. Noureddine, Ahmed Fawaz, illiam H. Sanders
Acknowledged Federal Support: **Y**

**Partners**

,

I certify that the information in the report is complete and accurate:
Signature: Andrea Whitesell
Signature Date: 4/19/22 12:37PM

INFORMATION TRUST INSTITUTE

# Information and Software Assurance: Resiliency, Security, and Trust in Complex Engineered Systems

Contract Number W911NF1310086

Final Report

Principal Investigator: David Nicol

Reporting Period: June 24, 2013 to June 23, 2019

# Contents

# Summary

This report is the cumulation of work funded by Army Research Office contract number W911NF1310086 for the period of performance of June 24, 2013 to June 23, 2019. There is a brief write up of each research project: accomplishments and personnel. Also included in this report are funded outreach events and a cumulative list of journal and conference publications.

## Project Title: Developing Security Science from Measurements

## Project Personnel: Ravi Iyer and Zbigniew Kalbarczyk

## Accomplishments:

We explored application of Linux containers (LXC), a light-weight alternative to Virtual Machines (VM), to build a security testbed, a controlled system and network environment where attacks can be replicated. The proposed testbed architecture is based on two virtualization technologies: Virtual Machine Monitors (VMM) at the hardware-level and Linux Containers (LXC) at the operating-system-level to emulate multiple isolated systems on a single control host.

### Security testbed

A security testbed is a controlled system and network environment where attacks can be replicated. The testbed architecture is based on two virtualization technologies: Virtual Machine Monitors (VMM) at the hardware-level and Linux Containers (LXC) at the operating-system-level to emulate multiple isolated systems on a single host. The testbed provides: i) isolation – to prevent an attack affecting production infrastructure, ii) instrumentation – to collect system and network events in various attack stages, and iii) repeatability of experiments and convenient redeployment and use by other security researchers.

### Isolation

While LXC creates an isolated system using process's models on a shared kernel, VMM provides an isolated system by spawning a full-featured virtual machine. Compared to VMM, LXCs are lightweight and can be used to replicate application-level attacks, e.g., an SQL injection attack in a web application or a buffer overflow vulnerability. VMMs can replicate kernel-level attacks, e.g., an integer overflow in a device driver. Instrumentation. We deploy various monitors across the system stack and network to collect events during the attacks. For example, we use kernel probes to collect kernel events, syslog and application logs to collect application events, and netflow to collect network events. Most of the monitors are deployed on the same system where we replay attacks. We also deploy monitors in separate containers or VMs when it is possible to prevent attackers from contaminating the monitors.

### Repeatability

Each attack is packaged using a group of containers or VMs that contain the system that the attack is run on and the corresponding monitors. We organize attacks into a centralized registry, where a security researcher can clone the attacks into their local machine for educational purpose. Monitoring data from the security testbed are constantly delivered to our probabilistic graphical model, i.e., AttackTagger, as feedbacks to improve attack detection.

## Risks/Areas of Concern:

Extracting the useful data from the large volume of data in security logs (e.g., IDS logs and syslogs) is time consuming and requires development of software tools to automate the data filtering and mining. In order to mitigate this problem we closely collaborate with the National Center for Supercomputing Applications security team on design of the right tools and identifying the data of interest.

## Project Title*:* Mathematical Foundations & Analysis Techniques for Protocol Indistinguishability

**Project Personnel:** Jose Meseguer and Santiago Escobar

## Accomplishments:

We have investigated three key topics:

1. Further theories of homomorphic encryption having the finite variant property, and experimentation in Maude-NPA to analyze protocols using such theories. Specifically, in [5] we have proved that homomorphic encryption over exclusive or (XOR) has the finite variant property, and have develop and documented a much more thorough experimental evaluation than the preliminary one summarized in the earlier manuscript [3] (where, furthermore, XOR was not studied) of various protocols using different homomorphic encryption theories in Maude-NPA.
2. Full proofs and full theoretical treatment of a mathematical theory of indistinguishability and its formal verification in Maude-NPA. As the project title indicates, this is the central research topic of this project. Furthermore, a thorough experimental evaluation of this technique on actual protocols has also been carried out. All this has been documented and submitted for publication to the ESORICS 2014 Conference in [6].
3. Development of a theory of variant narrowing and generalization of the finite variant property for conditional equational theories. This is a key advance in the theoretical foundations of Maude-NPA, since it will substantially broaden the class of equational cryptographic theories that can be analyzed. An advanced draft has been developed and we plan to submit it for publication in July 2014.

## Risks/Areas of Concern*:*

One clear area of concern all along has been that we only had one year to advance a three- year project. As documented in the list of publications, within the limited time and limited resources available, key objectives have been accomplished and we have reached a very good basis to achieve many others. However, their accomplishment will not be possible, since this project was not continued under this funding.

## Project Title: Trust from Explicit Evidence: Integrating Digital Signatures and Formal Proofs

## Project Personnel: Elsa L. Gunter

## Accomplishments:

1. Wrote out type system corresponding to prototypes
    - ❖ Carried out proofs of correctness
2. Added affine channels to language
    - ❖ Affine channels are needed to conveniently represent “data structure” like services (removes need to manually free such services)
    - ❖ Proof of Affine Weakening in our type system
        i. Needed to confirm that “affine” channels truly are affine
    - ❖ Proof that type system prevents affine services from using linear channels
        i. Means we won’t accidentally “lose” linear services and violate our guarantee that linear services are fully consumed
        ii. Justifies recursively terminating services that affine services use
3. Subtyping proofs
    - ❖ Subtyping is how we expressed different levels of access
    - ❖ While working on proving our subtyping correct, discovered some subtly wrong interactions with polymorphism
        i. Solution suggested by Sekiguchi and Yonezawa 94
        ii. Proofs ongoing
        iii. If successful, may trade higher-quality bidirectional error messages for inferability
4. Solo Semantics
    - ❖ Prior work on asynchronous semantics added non-blocking output
    - ❖ Solo calculus suggests we may want non-blocking input as well
    - ❖ Seems to correspond to sending futures in the shared memory case
    - ❖ When distributed, less clear if we can allow for maximal delay
5. Adjoint Logic
    - ❖ The presentation of the full type system is bulky
    - ❖ Adjoint logic suggests that by splitting our modalities into half-modalities we can simplify the rules somewhat
    - ❖ Investigated, but proofs were done with larger system, unclear if switching would be desirable long term

6. Mix
    - ❖ Allows for non-interacting parallel systems
    - ❖ A partial answer to “Why don’t you have a general parallel construct like my favorite formalism?”
7. Silent One Left Rule
    - ❖ Treat completed linear channels nearly like they’re affine
    - ❖ Allows us to omit some unneeded bookkeeping
    - ❖ Explored different trade-offs between predictability of silent 1L execution and performance (qualitative)

## Tools:

1. LiquidPi: Designed, implemented, and proved correct a system (LiquidPi) that integrates Honda’s Session Types that describe the behavior of distributed systems with the automatically inferable dependent types of Rondon. This system should allow us to automatically check that distributed programs written in our language conform to security specifications.
2. SILL:
    - ❖ 1. Implemented the core of SILL that includes bidirectional type checking for monadic linear session types with infinite recursive types and branching subtyping efficiently; a modular interpreter featuring selectable threading/forking for handling concurrency and selectable asynchronous communication; a new equivalent (more efficient) semantics for SILL’s forwarding construct; and cryptographic primitives and explicit dynamic type checking constructs.
    - ❖ Implemented a bidirectional type checker that can be expanded to more expressive data types; a modular backend interpreter allowing for selectable evaluation strategy with high amounts of code reuse; improved parser/ lexer error reporting.
    - ❖ Designed the theory and implemented support for register/request primitives for communication with servers having persistent store.
    - ❖ Provided theory and implementation of a merge of linear and affine types for communication channels, allowing for the representation of persistent data structures associated with services, but with guarantees that affine services will not use linear channels (which have stronger usage guarantees).

## Risks/Areas of Concern:

Because of the early termination / reduction of funding, the third phase of our project, the usability study, was not accomplished.

## Project Title: Classification of Cyber-physical System Adversaries

## Project Personnel: Sayan Mitra, Geir Dullerud, Rayaduram Srikant, and Sibin Mohan

### Accomplishments:

1. Journal version of paper in preparation “Differential Privacy of Distributed Linear Feedback Systems”, Yu Wang, Zhenqi Huang, Sayan Mitra, and Geir Dullerud, March 2015.
2. New paper: Zhenqui Huang, Sayan Mitra, and Nitin Vaidya, “Differentially Private Distributed Optimization”, In IEEE International Conference on Distrusted Computing and Networks (ICDCN), 2015.
3. New paper: “Entropy-minimizing Mechanism for Differential Privacy of Discrete-time Linear Feedback Systems”, Wang, Yu, Huang, Zhenqi, Mitra, Sayan, and Dullerud, Geir. In Conference on Decision and Control (CDC) 2014.
4. New paper submitted: Huang, Fan, Mereacre, Mitra, and Kwiatkowska, “Simulation Based Verification of Implantable Medical Devices with Guaranteed Coverage”, submitted for review, 2014.
5. Presentation at Information Trust Institute TSS seminar series: Static and Dynamic Analysis of Security Metrics for Cyber-Physical Systems by Sayan Mitra February 2015.
6. We have disseminated the research results from this project through presentations at several International Conferences (IEEE CDC, ICDCN, CAV, HSCC), and invited lectures (UC Berkeley, Georgia Tech, University of Michigan).
7. Building-up on our algorithms and tool for bounded time reachability computation for nonlinear and hybrid systems, in the past couple of months we have focused our energies on developing an algorithm for analyzing nondeterministic models with adversaries. The preliminary results from the work in progress are promising and we are preparing a working paper for submission.
8. New result on compositional approximation of reach sets of hybrid models using modular simulations. Given N component hybrid automata models n dimension each, we show that it is possible to compute arbitrarily precise reach set over-approximations using a reduced system of N dimensions and simulations of the original system. The method easily scales to Nn = 40 dimensional systems and can be used to bound the effects of adversarial inputs to the system. The results (see Table 1 below) are going to appear in: Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells, Z. Huang, C. Fan, A. Mereacre, S. Mitra, and M. Kwiatkowska. To appear in Computer Aided Verification (CAV), LNCS, 2014.
9. We have developed techniques for proving abstraction relations between dynamical system models. These abstractions can capture models of adversaries and give a measure of how tolerant the system is for a given type of adversary.
10. On Price of Privacy in Distributed Control Systems by Zhenqi Huang, Yu Wang, Sayan Mitra, and

Geir Dullerud, appeared in in The 3rd ACM International Conference on High Confidence Networked Systems (HiCoNS) to be held April 15-17, 2014 in Berlin, Germany as part of Cyber Physical Systems Week 2014 (CPSWeek 2014).

11. The paper Proofs from Simulations and Modular Annotations by Zhenqi Huang and Sayan Mitra was nominated for Best Student Paper Award at CPSWeek conference HSCC 2014.
12. Master's thesis: "Verification of Nonlinear Hybrid Systems with Simulation Traces and Compositional Reasoning", Zhenqi Huang, August 2013. • Zhenqi Huang participated in the Summer School on formal methods for security at University of Illinois at Urbana Champaign in 2013.
13. Master's thesis: Stability of Linear Autonomous Systems under Regular Switching Sequences, Yu Wang, July 2014.
14. Established a lower-bound for accuracy of convergence for a given level of privacy, for the building block problem of synchronous iterative consensus problem.
15. Generalized the synchronous mechanism to work in asynchronous and distributed networks for solving private consensus.
16. Switched system analysis and synthesis for worst-case models; initiated work on parallel algorithms for determining optimally-secure policies.
17. Stanley Bak, Fardin Abdi Taghi Abad, Zhenqi Huang, Marco Caccamo. Using Run-Time Checking to Provide Safety and Progress for Distributed Cyber-Physical Systems. To appear in IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA2013), 2013. 2. Journal paper submitted: Control of Linear Switched Systems with Receding Horizon.
18. Modal Information by Raymond Essick, Ji-Woong Lee and Geir Dullerud, appeared in IEEE Transactions on Automatic Control, 2014.
19. Conference paper submitted: Receding Horizon Control for Path-by-Path LQG Performance by Raymond Essick, Ji-Woong Lee and Geir Dullerud; appeared in American Control Conference (ACC), 2013. Dissemination of the results
20. Proofs from Simulations and Modular Annotations Presented by Zhenqi Huang at the 17th International Conference on Hybrid Systems: Computation and Control, nominated for DENSO Best Student Paper Award.
21. On Price of Privacy in Distributed Control Systems Presented by Zhenqi Huang at the 3rd ACM International Conference on High Confidence Networked Systems (HiCoNS).
22. Algorithmic analysis of Cyberphysical Systems, Invited talk by Sayan Mitra, at Georgia Institute of Technology, April 2014.
23. Differentially Private Iterative Synchronous Consensus. Presented by Zhenqi Huang at the Workshop on Privacy in the Electronic Society collocated with CCS at Raleigh, October 2012. Presented by Sayan Mitra as a poster at the SoS Community meeting, November 2012.

## Project Title: Toward a Theory of Resilience in Systems: A Game-Theoretic Approach

## Project Personnel: M. Tamer Basar and Quanyan Zhu

## Accomplishments:

The security and resilience of modern infrastructures require an interdisciplinary research effort to investigate security mechanisms and develop tools for analyzing and designing complex systems to achieve inter-and intra-layer resilience. Game-theoretic approaches adopted in our research allow us to adopt a holistic viewpoint toward designing systems of multi-layer interactions, contributing toward the development of a science of security and resilience. Our research is also motivated by many emerging complex networked systems, such as those in health care, biomedicine, smart power grid, and transportation systems, as well as social networks.

The papers listed below are based on our research on resilience and secure collaboration. They all have either publication or completion (and submission) dates that fall within the current quarter. A description of the contents of each paper is given below.

Paper [1]:

In this work, we consider a minimax control problem for linear time-invariant (LTI) systems over unreliable communication channels. This can be viewed as an extension of the **H**-infinity optimal control problem, where the transmission from the plant output sensors to the controller, and from the controller to the plant are over sporadically failing channels. We consider two different scenarios for unreliable communication. The first one is where the communication channel provides perfect acknowledgments of successful transmissions of control packets through a clean reverse channel, that is, the TCP (Transmission Control Protocol). Under this setting, we obtain a class of output feedback minimax controllers; we identify a set of explicit threshold-type existence conditions in terms of the **H**-infinity disturbance attenuation parameter and the packet loss rates that guarantee stability and performance of the closed-loop system. The second scenario is one where there is no acknowledgment of successful transmissions of control packets, that is, the UDP (User Datagram Protocol). We consider a special case of this problem where there is no measurement noise in the transmission from the sensors. For this problem, we obtain a class of corresponding minimax controllers by characterizing a set of (different) existence conditions. We also discuss stability and performance of the closed-loop system, illustrating the results in all cases with extensive simulations.

Paper [2]:

With increasing integration of information technologies into industrial systems and networks, such as the power grid, robust and resilient control system design is essential for assuring the robust performance of

cyber-physical control systems in the face of adversarial attacks. We present in this article a hybrid game-theoretic framework whereby the occurrence of unanticipated events is modeled by a stochastic switching, and deterministic uncertainties are represented by disturbances lying within known ranges. The design of a robust controller at the physical layer takes into account risks of failures due to the cyber system, while the design of the security policies is based on its potential impact on the control system. The cross-layer coupled design introduced in this article results in solving a zero-sum differential game for robust control coupled with a zero-sum stochastic game for the security policy. The two games are intertwined and coupled together through cyber and physical system variables. The solution to the coupled games requires a zooming-in process, which uses variables from the cyber level to solve the physical layer game, and a zooming-out process, which uses physical system variables to solve the cyber layer game. The joint design results in a robust and resilient controller switching between different modes for guaranteeing performance in the face of unexpected events.

Paper [3]:

In this paper, we formulate a three-player three-stage Colonel Blotto game, in which two players fight against a common adversary. We assume that the game is one of complete information, that is, the players have complete and consistent information on the underlying model of the game; further, each player observes the actions taken by all players up to the previous stage. In the first stage, players can add additional battlefields. In the second stage, the players (except the adversary) are allowed to transfer resources among each other if that leads to improvement in their expected payoffs, and simultaneously, the adversary decides on the amount of resource it allocates to the battle with each player subject to its resource constraint. At the third stage, the players and the adversary fight against each other with updated resource levels and battlefields. We compute the subgame-perfect Nash equilibrium for this game. Further, we show that when playing according to the equilibrium, there are parameter regions in which (i) there is a net positive transfer, (ii) there is absolutely no transfer, (iii) the adversary fights with only one player, and (iv) adding battlefields is beneficial to a player. In doing so, we also exhibit a counter-intuitive property of Nash equilibrium in games: extra information to a player in the game does not necessarily lead to a better performance for that player. The result finds application in resource allocation problems for securing cyber-physical systems.

Paper [4]:

In this paper, we analyze stability properties of a susceptible-infected-susceptible (SIS) diffusion model over directed networks. Similar to the majority of infection-spread dynamics, our model exhibits a threshold phenomenon. When the curing rates in the network are sufficiently high, the *all-healthy* state is globally asymptotically stable. Otherwise, a strictly positive endemic state arises and the entire network could become infected. Using notions from positive systems theory, we prove that the endemic state is globally asymptotically stable in strongly connected networks. For the case when the graph is weakly connected, however, we provide conditions for the existence, uniqueness, and global stability of a strictly positive

endemic state. Moreover, for the case when the curing rates are low, we develop a framework for reducing the residual infection in directed infected networks using a limited number of controllers. Several simulation studies illustrate our results.

Paper [5]:

In this paper, we formulate a three-player three-stage Colonel Blotto game, in which two players fight against a common adversary. We assume that the game is one of complete information, that is, the players have complete and consistent information on the underlying model of the game; further, each player observes the actions taken by all players up to the previous stage. The setting under consideration is similar to the one considered in our paper [4] below, but with a different information structure during the second stage of the game; this leads to a significantly different solution.
In the first stage, players can add additional battlefields. In the second stage, the players (except the adversary) are allowed to transfer resources among each other if it improves their expected payoffs, and simultaneously, the adversary decides on the amount of resource it allocates to the battle with each player subject to its resource constraint. At the third stage, the players and the adversary fight against each other with updated resource levels and battlefields. We compute the subgame-perfect Nash equilibrium for this game. Further, we show that when playing according to the equilibrium, there are parameter regions in which (i) there is a net positive transfer, (ii) there is absolutely no transfer, (iii) the adversary fights with only one player, and (iv) adding battlefields is beneficial to a player. In doing so, we also exhibit a counter-intuitive property of Nash equilibrium in games: extra information to a player in the game does not necessarily lead to a better performance for that player. The result finds application in resource allocation problems for securing cyber-physical systems.
Paper [6]:

In this paper, we study the problem of aggregator's mechanism design for controlling the amount of active, or reactive, power provided, or consumed, by a group of distributed energy resources (DERs). The aggregator interacts with the wholesale electricity market and through some market-clearing mechanism is incentivized to provide (or consume) a certain amount of active (or reactive) power over some period of time, for which it will be compensated. The objective is for the aggregator to design a pricing strategy for incentivizing DER's to modify their active (or reactive) power consumptions (or productions) so that they collectively provide the amount that the aggregator has agreed to provide. The aggregator and DERs' strategic decision-making process can be cast as a Stackelberg game, in which aggregator acts as the leader and the DERs are the followers. In a recent earlier work, we had introduced a framework in which each DER uses the pricing information provided by the aggregator and some estimate of the average energy that neighboring DERs can provide to compute a Nash equilibrium solution in a distributed manner. Here, we focus on the interplay between the aggregator's decision-making process and the DERs' decision-making process. In particular, we propose a simple feedback-based privacy-preserving pricing control strategy that allows the aggregator to coordinate the DERs so that they collectively provide the amount of

active (or reactive) power agreed upon, provided that there is enough capacity available among the DERs. We provide a formal analysis of the stability of the resulting closed-loop system. We also discuss the shortcomings of the proposed pricing strategy, and propose some avenues of future work. We illustrate the proposed strategy via numerical simulations.

Paper [7]:

This paper considers a minimax control problem over multiple packet dropping channels. The channel losses are assumed to be Bernoulli processes, and operate under the transmission control protocol (TCP); hence acknowledgments of control and measurement drops are available at each time. Under this setting, we obtain an output feedback minimax controller, which is implicitly dependent on rates of control and measurement losses. For the infinite-horizon case, we first characterize achievable H-infinity disturbance attenuation levels, and then show that the underlying condition is a function of packet loss rates. We also address the converse part by showing that the condition of the minimum attainable loss rates for closed-loop system stability is a function of H-infinity disturbance attenuation parameter. Hence, those conditions are coupled with each other. Finally, we show the limiting behavior of the minimax controller under the disturbance attenuation parameter.

Paper [8]:

In this paper, we analyze stability properties of a susceptible-infected-susceptible (SIS) diffusion model over directed networks. Similar to the majority of infection-spread dynamics, our model exhibits a threshold phenomenon. When the curing rates in the network are sufficiently high, the *all-healthy* state is globally asymptotically stable. Otherwise, a strictly positive endemic state arises and the entire network could become infected. Using notions from positive systems theory, we prove that the endemic state is globally asymptotically stable in strongly connected networks. For the case when the graph is weakly connected, however, we provide conditions for the existence, uniqueness, and global stability of a strictly positive endemic state. Moreover, for the case when the curing rates are low, we propose a framework for reducing the residual infection in directed infected networks using a limited number of controllers. Several simulation studies illustrate our results.

Paper [9]:

In this paper we consider a class of games known as Colonel Blotto games, which were first introduced in a military context, but now have applications in security of cyber-physical systems. What we consider is an extension of the classical Colonel Blotto game to three stages and three players, and with complete information. The scenario is one where two of the players collaborate (form a common front and fight) against a third player (called the adversary). Each player is endowed with a certain amount of resources at the beginning of the game, and the number of battlefields on which a player and the adversary fight is specified. The first two players are allowed to form a coalition if it improves their payoffs. In the first stage, the first two players may add battlefields at some cost. In the second stage, the first two players may

exchange resources (transfer from one player to the other). The adversary observes this transfer, and decides on the allocation of its resources to the two battles with the players. At the third step, the adversary and the other two players fight on the updated number of battlefields and receive payoffs. In the paper, we characterize the subgame-perfect Nash equilibrium (SPNE) of the game in various parameter regions. In particular, we show that there are certain parameter regions in which if the players act according to the SPNE strategies, then either (i) one of the first two players add battlefields and transfer resources to the other player (a coalition is formed), or (ii) there is no addition of battlefields and no transfer of resources (no coalition is formed). We discuss in the paper the implications of these results on resource allocation for securing cyber-physical systems.

Paper [10]:

In this paper, we analyze the stability properties of a dynamical system that describes the evolution of the probability of infection in a network. We show that this model can be viewed as a concave game among the nodes. This characterization allows us to provide a simple condition that can be checked in a distributed fashion, for stabilizing the origin. When the curing rates at the nodes are low, a residual infection stays within the network. Using properties of Hurwitz Mertzel matrices, we show that the residual epidemic state is locally exponentially stable. We also demonstrate that this state is globally asymptotically stable (GAS). Furthermore, we investigate the problem of stabilizing the network when the curing rates of a limited number of nodes can be controlled. In particular, we characterize the number of controllers required for a class of undirected graphs. Several simulations demonstrate our results.

Paper [11]:

This paper considers a minimax (**H**-infinity) control problem for linear time-invariant (LTI) systems where the system dynamics and the measurement process are affected by unknown disturbances (possibly controlled by an adversary) and the communication loop relies on a TCP-like packet-dropping network. The problem is formulated within a zero-sum dynamic game framework, with the packet-dropping network governed by two independent scalar Bernoulli processes that model control and measurement packet losses. A complete solution (a robust output feedback minimax controller) is obtained in the paper. The paper also considers the infinite-horizon case. Necessary and sufficient conditions are provided in terms of the packet loss rates and the **H**-infinity disturbance attenuation parameter, under which the minimax controller exists and is able to stabilize the closed-loop system. In particular, we show that unlike the case when the disturbances have Gaussian statistics, these conditions are coupled and therefore cannot be satisfied independently.

## Project Title: Scalable Methods for Security against Distributed Attacks

## Project Personnel: Gul Agha, Kirill Mechitov, and Peter Dinges

## Accomplishments:

1. Knowing inputs that cover a specific branch or statement in a program is useful for debugging and regression testing. Symbolic backward execution (SBE) is a natural approach to find such targeted inputs. However, SBE struggles with complicated arithmetic, external method calls, and data-dependent loops that occur in many real-world programs. We developed *symcretic execution*, a novel combination of SBE and concrete forward execution that can efficiently find targeted inputs despite these challenges. An evaluation of our approach on a range of test cases shows that symcretic execution finds inputs in more cases than concolic testing tools while exploring fewer path segments. Integration of our approach will allow test generation tools to fill coverage gaps and static bug detectors to verify candidate bugs with concrete test cases. The approach could be particularly useful in concurrent programs by narrowing the number of likely schedules that need to be considered—schedules which do not cause an access to a particular potentially problematic command in a specific actor need not be considered.

2. Latent *Heisenbugs*, caused by interleaving of messages (representing object access patterns) that have not been previously observed, are a key source of security breaches. We have been developing techniques to identify and/or prevent such bugs with a focus on probabilistic methods. We developed a method for the holistic behavioral analysis of concurrent software to expose its concurrency structure. Data is often connected through invariants and must be updated together to maintain data consistency. For example, at the level of a data field, the value of the size field of a list object must equal the number of elements in the array that stores the list entries. Interleaved access to such fields from concurrent threads can expose or produce an inconsistent state in the object containing those fields. High-level data races may be prevented with control centric synchronization mechanisms such as locks. However, to protect a group of data fields, the programmer must recognize all execution paths that result in problematic interleavings, and use locks to prune them. This requires complicated non-local reasoning over all possible execution paths. An alternative is to use data-centric synchronization which localizes the reasoning. Annotating the code to ensure data-centric synchronization can prevent harmful interleaved access to fields in the same semantic unit. This reduces the potential for high-level data races on execution paths that the programmer may not have conceived of. This enables checking for consistency and deadlock-freedom.

3. We implemented a tool to identify data invariants in Java programs. The tool uses probabilistic reasoning over traces that were successful in testing phase of a program to identify highly likely

data field invariants. The use of probabilistic reasoning avoids unnecessarily constricting the available concurrency in a program because of an artifact of randomness in observations. The tool was successfully applied to a corpus of programs.

4. Finding potential security violations can be facilitated by analyzing programs for vulnerabilities. Some statements can be identified as potential problems if executed under certain data input or scheduling conditions. In the course of our research, we identified an issue with test input generators. The state of the art test generators such as Microsoft's Pex tool (resulting in part from our own research several years ago) use concolic execution. Concolic execution relies in part on solving path conditions to systematically explore a program and generate high coverage tests. However, programs may contain complex arithmetic path conditions, which may be undecidable. Existing test generators either simplify such constraints with concrete values to make them decidable, or rely on strong but incomplete constraint solvers. Unfortunately, simplification yields coarse approximations whose solutions rarely satisfy the original constraint; and constraint solvers cannot handle calls to native library methods. We show how a simple combination of linear constraint solving and heuristic search can overcome these limitations. On a corpus of 11 programs, our *Concolic Walk* algorithm generates tests with two- to three-times higher coverage than simplification-based tools while being up to five-times as efficient. Furthermore, our algorithm improves the coverage of two state-of-the-art test generators by 21% and 32%. Other concolic and symbolic testing tools could integrate our algorithm to solve complex path conditions without having to sacrifice any of their own capabilities, leading to higher overall coverage in a scalable testing tool.

## Project Title: Science of Human Circumvention of Security (SHuCS)

## Project Personnel: Jim Blythe, Ross Koppel, Sean Smith

## Accomplishments:

1. The team (minus Blythe) met for a face-to-face workshop in July and discussed the ongoing DASH simulation work, the survey work, our corpora of workarounds and other IT mismatches (now up to about 300), and our analysis of that based on the semiotic framework we used in the earlier *JAMIA* paper.
2. The *JAMIA* paper by Smith and Koppel on usability problems with health IT (pre-SHUCS, but related) received another accolade, this time from the International Medical Informatics Association, which also named it one of best papers of 2014. We are updating that paper to include discoveries from our analysis of the workaround corpora above.
3. At the *2014 USENIX Summit on Health Information Technologies* (August 2014), all three PIs, along with PhD student V. Kothari, presented "Ethnography of Computer Security Evasions in Healthcare Settings: Circumvention as the Norm" on our work. In addition, PI Koppel gave the keynote "Software Loved by its Vendors and Disliked by 70% of its Users: Two Trillion Dollars of Healthcare Information Technology's Promises and Disappointments."
4. PI Koppel presented. "Ethnography of Computer Security Evasions in Healthcare Organizations: Circumvention of Cyber Controls" (Koppel, Blythe, Smith) at the *European Sociological Association Midterm Conference* in August.
5. The team also submitted a paper to the *2015 IEEE International Symposium on Technologies for Homeland Security*, which has been accepted.
6. Dartmouth Ph.D. student Vijay Kothari continued working on the project. He continued exploring DASH models with PI Blythe, with an eye towards choosing the scenarios to model in a multi-agent setting, the hypotheses to initially explore, and how to validate the resulting models. (Many of these questions were prompted by feedback from our initial modeling paper [1].) Student Kothari also started exploring the usability and security literature for additional relevant work.
7. PI Blythe continued working on modeling BCMA workarounds in DASH. PI Smith mined the literature and ideas unearthed during his winter-term "Special Topics" class for circumvention scenarios and motivations. PI Koppel has continued his work with surveys and interviews.
8. The team is exploring using NLP/automatic text analysis on problem reports and change logs from partner IT departments (unearthed during our fieldwork), and also using these techniques on the open-ended responses to our questionnaire.
9. PI Blythe presented our agent paper [1] at *ACySE* in May; PI Koppel will be presenting "Ethnography of Computer Security Evasions in Healthcare Organizations: Circumvention of Cyber

Controls" (Koppel, Blythe, Smith, Kothari) at the *European Sociological Association Midterm Conference* in August. The team also has a panel proposal pending for *Usenix HealthTech*.

10. The *JAMIA* paper by Smith and Koppel on usability problems with health IT (pre-SHUCS, but related) was named "among most significant papers of the year." We are updating that paper to include: mental models of: payers (key), administrators, patients, and to include circumvention triggers.
11. Via fieldwork in real-world enterprises, we have been identifying and cataloging types and causes of circumvention by well-intentioned users. We are using help desk logs, records security-related computer changes, analysis of user behavior in situ, and surveys---in addition to interviews and observations. We then began to build and validate models of usage and circumvention behavior, for individuals and then for populations within an enterprise.
12. We published a preliminary report about the general project in *IEEE Security and Privacy* [2], and a preliminary paper on our agent-based modeling work [1]; we also had three additional conference presentations (two at *HealthTech* and one at the *European Sociological Association*).

## Project Title: Quantitative Assessment of Access Control in Complex Distributed Systems

## Project Personnel: David Nicol and Mouna Bamba

## Accomplishments:

1. Putting finishing touches on new capabilities and analysis integrated into a useable framework.
2. We completed a prototype of a system that, given hosts and vulnerabilities, computes the vulnerability of the system to stepping stone attacks through the given hosts. We would find hosts in vulnerability scan data, and manually include into the network model. For the remainder of the project we aim to make this capability more useable by automating the integration of new topological elements discovered by observation (not just configuration) into the model. Our first step this path was to develop and test new algorithms for merging topological information into a system data structure. Initial testing proved its utility straightaway, by identifying bugs in the previous approach.
3. Infrastructure, algorithm, and theoretical development finally came together. Theory: We formalized the problem of identifying the k "easiest" stepping stone attacks in a network as a graph path discovery problem, where nodes represent hosts with vulnerable services and a (directed) edge indicates that an attacker at the source is permitted to access some vulnerable service at the destination. The edge is labeled with a difficulty weight, but the model takes into account two salient features: a) The difficulty of exploiting a vulnerability may be less if the attacker has exploited that same vulnerability before, and b) The difficulty of exploiting a vulnerability may be greater, if an earlier exploit was detected and the defender raises additional defenses. In our model then the cost of a stepping-stone attack is represented as a path through the graph, and the difficulty of the attack is the sum of the edges on the path. However, an edge weight is permitted to depend on the path prefix leading to it. We have proven that under this model the problem of finding a least-cost stepping stone attack from a given attacker location to a given victim location is NP-Hard, a result of interest mostly because it validates the utility of examining heuristics (such as we have been doing) based on Monte Carlo sampling, where the sampling is skewed in directions "likely" to lead to low cost paths. This result is also interesting in the context of the significant result in attack graph analysis which shows that if an attack graph is "monotone" (meaning that an attacker never loses privileges in the course of an attack) then the existence of a successful attack can be determined in polynomial time, whereas without that assumption the problem is NP-Complete. Our result, applied to monotone attacks and even the case where attacks may become easier, shows that asking a question about difficulty of attack rather than just existence can push the problem back into the realm of intractable problems. Algorithm: We developed an algorithm that stochastically samples "the next" vulnerability to exploit in path exploration based on estimated shortest distances from the set of potential next

steps, where the estimate is based on the assumption that edge costs do not change from whatever values they have at the point the sampling is done, and have a parameter in the shaping of that distribution which can vary it from being uniformly random, to essentially deterministic in choosing the path with estimated least remaining cost. We find (so far only empirically) that a balance is needed when one is seeking more than one low cost path, for the deterministic end makes it hard to find more than one low cost path, and the uniform selection ends up finding too many long paths. We are working on a less heuristic basis for the selection.
Infrastructure: The NP-View tool has been augmented with capabilities which make all of this practical. NP-View first computes the connectivity between hosts, identifying which ports and protocols are involved. The results of an nmap scan are integrated so that these hosts are augmented with discovered open ports and services. CVSS scores are then accessed and incorporated into the model, and a multi-graph such as described in the Theory section is built, with the algorithm discussed earlier applied. Much of this work is reported in a paper "Modeling and Analysis of Stepping Stone Attacks", which will appear in the 2014 Winter Simulation Conference (and which will be sent to NSA when the camera-ready version is finished later in June).

## Project Title: Quantitative Security Metrics for Cyber-Human Systems

## Project Personnel: William H. Sanders, Michael Ford, and Ken Keefe

### Accomplishments:

Began design of Mobius execution visualization and debugging framework extensions for the Human-Influenced Task-Oriented Process (HITOP) formalism.

To evaluate how humans act and react within a complex system, we must model many aspects of human activities, including ones related, for example, to education, training, decision-making, and human performance. We group all those areas under the single subject heading of “human performance and decision-making.” Perhaps obviously, human performance and decision-making have been studied in a variety of fields because of their importance to the outcomes of many systems.

Human-machine systems are the basis for many types of technology, and their development is often impelled by the desire to make human tasks easier. Relevant fields of study involving human-machine systems include human-computer interaction, human factors, and various branches of engineering.

Task analysis is a method, used in many fields, by which human activities can be decomposed into sets of tasks. Tasks are associated with sets of internal characteristics and external conditions that affect performance. Task analysis provides an important tool for breaking a general system down into a set of important tasks and documenting the conditions related to the performance of the tasks.

We adopt the ideas that human activities can be represented and modeled as a set of tasks within a process; that task performance can be modeled relative to a goal and using a set of possible task operations; and that humans within a complex system must be explicitly modeled in order to adequately characterize system performance. We add to the earlier work our approach of defining a cyber-human system model and the relationships between model elements with the opportunity-willingness-capability ontology. We use all of those ideas to construct process models for our solution method.

We have chosen to implement our model as a process model. Process models are formalized descriptions of activities within a process. Process models are often used in process engineering to model physical and/or industrial processes, e.g., the production of steel. Process models are also used to model informational and/or business processes; such models are typically referred to as business process models.

Cyber security models are increasingly being used as a means to understand, measure, and predict how a system will perform relative to various cyber security metrics. Most cyber security models and tools fall into two categories: system-based models and attacker-based models. We argue that model-based

evaluation of cyber security is a useful approach and that integrated system models of humans and computer systems can provide valuable tools for system analysis with respect to cyber security. We have added to this body of work our approach, which is to build an integrated model of human users and computer systems, i.e., an approach that uses user-system hybrid models.

To describe how we model the effects of human behaviors, especially human decisions, on a system, we have defined our conceptual model of the cyber-human system (CHS). That is, we have described how a cyber-human system may be decomposed into, or represented by, sets of model element types specific to our aim. In its most basic sense, a CHS is a system in which the decisions and actions of humans in relation to computers affect measurable and important system outcomes.

Examples of such systems include typical business or academic settings in which system users must interact with an IT infrastructure, industrial settings in which workers must interact with computer-based process control systems, or something as simple as a cell phone and its user. For each of these examples, a CHS model may be created to analyze how humans perform tasks, achieve goals, and affect outcomes within the overall system.

Our conceptual model divides CHS elements into four types: components, participants, processes, and tasks. We assume that all relevant CHSs, plus their desired properties, can be represented using these element types. Components are the physical objects that make up a system. Participants are the entities that initiate and perform actions within a system. Processes are ordered arrangements of activities that specify how the system is used and are usually associated with some purpose or goal. A task is an atomic unit of work that is carried out by a resource, where a resource is one or more participants using one or more components.

All actions within a CHS model occur in terms of tasks, and it is therefore necessary to specify what system states can lead to task performance and how the outcomes of task performance may be affected by these states. We do so by using a formal naming system, the opportunity-willingness-capability (OWC) ontology, to associate sets of CHS elements with each task. Simply put, the OWC ontology classifies a set of CHS elements conditioned on how these sets of elements affect task performance.

Opportunity exists for a task, if the necessary and sufficient conditions are available to attempt task performance. Willingness exists for a task if a participant has the desire to perform a task. A willingness state is only applicable to tasks performed by humans. Capability exists for a task if a participant can, i.e., has the ability, to perform a task such that one of a set of mutually exclusive outcomes can be achieved.

The OWC ontology is useful in at least two ways. First, during the model definition phase, the OWC ontology provides a structured way of defining and grouping model elements for each task. For example, to model a process, we typically first decompose the process into an ordered arrangement of tasks [45],

[46]. While defining each task from the process decomposition, the analyst can directly define other related model elements and element states by listing the task's OWC elements. That provides a "ground-up" approach to defining a model that is intuitive and also guarantees the minimal state definition for each task.

Second, the OWC ontology speeds up model execution. Only those elements defined by the OWC ontology as related to a task are evaluated for changes when each task is evaluated for execution. That implies a smaller state space to search relative to each task and contributes to simulation efficiency.

## Project Title: End-to-end Analysis of Side Channels

## Project Personnel: Nikita Borisov

### Accomplishments:

- We performed an initial security analysis of our scheme and showed a dramatic reduction in the ability to perform website fingerprinting.
- These results will be presented in a poster at ACM CCS.
- Developed proxy-based website fingerprinting defense based on combining a web page into a single object.
- Evaluated the performance of the proxy-based defense and showed that it in fact improves performance over regular web page downloads.

See publications list for research results.

## Project Title: Secure Platforms via Stochastic Computing

## Project Personnel: Naresh Shanbhag, Rakesh Kumar, and Joseph Sloan

## Accomplishments:

We have shown with two example applications - boolean satisfiability (SAT) and sorting - how applications can be cast as Markov Chain algorithms and demonstrated their robustness to transition errors with rates as high as 40%. This quarter we attempted to understand how this approach ("stochastic inference") compares to the 'classical inference' approach. The comparison is important as there are some works that talk about inherent robustness in applications that use classical inference (e.g., Belief Propagation based LDPC decoder). We spent some time understanding how problems are represented as factor graphs and how classical inference works. We focused mainly on belief propagation. We looked at three applications: SAT, LDPC decoding and stereo matching. For SAT, we observed that BP does not converge often and it becomes worse as the number of variables increase or the hardness of the problem increases (in terms of clause to variable ratio). We found that BP version of LDPC deciding showed gradual degradation in performance (bit error rate) up to a fault rate of about 3x10^-4 for certain floating point errors. We are yet to inject fault into stereo-matching.

The next goal is to understand BP for stereo-matching and develop techniques to paralleilize Markov Chains.

- We propose a novel algorithmic approach to building attack-tolerant applications - by transforming applications into Markov chain algorithms. For such algorithms, many injection attacks may appear to be simply adding randomness to a process that is inherently random.
- We developed techniques for algorithmic error localization and partial recomputation and studied their scalability within the context of a parallel linear solver application (CG).
- We studied the robustness of inference-based implementations of computational problems.

## Project Title: Theoretical Foundations of Threat Assessment by Inverse Optimal Control

## Project Personnel: Tim Bertl and Navid Aghasadeghi

## Accomplishments:

- We have established a theoretical framework for inverse optimal control in the context of differentially flat systems (e.g., a quadrotor helicopter, a "five-link biped" model of human locomotion). This result has led to a breakthrough in our work on control of lower-limb prosthetic devices. Previously, it took a clinician four hours to hand-tune these devices for each patient. With our approach based in inverse optimal control, it takes two minutes (more than 100x speed-up).

  N. Aghasadeghi, H. Zhao, L. Hargrove, A. Ames, E. Perreault, and T. Bretl, "Estimation of Impedance Controller Parameters for Biped Locomotion," a full-length paper, to appear at the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2013.

- We compared our method of inverse optimal control to three prior methods, in the context of deterministic continuous-time nonlinear systems. Results show that our method performs better than and is more computationally efficient than prior methods.

  M. Johnson, N. Aghasadeghi, and T. Bretl, "Inverse optimal control for deterministic continuous-time nonlinear systems," a full-length paper, to appear at the IEEE Conference on Decision and Control, 2013.

- We derived a new approach to modeling human walking paths (viewed from above). We represent these paths as geodesics and apply max-margin structure learning to recover a cost function that would have produced an observed collection of geodesics. We have so far applied this approach to the design of a brain-machine interface for mobile robot navigation:

  A. Akce, J. Norton, and T. Bretl, "A brain-machine interface to navigate mobile robots along human-like paths amidst obstacles," a full-length paper, presented at the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2012.

- We have established a theoretical framework that allows us to characterize the space of solutions to deterministic, continuous-time optimal control problems. We have shown that for a broad class of such problems, the set of local optima is a smooth manifold of finite dimension that can be parameterized by a single (global) coordinate chart. This geometric result provides a rigorous foundation for our approach to threat assessment (which will be developed in the coming months). It has also led to breakthroughs in other areas, e.g., long-standing problems in robotic manipulation of deformable objects:

  T. Bretl and Z. McCarthy, "Equilibrium configurations of a Kirchhoff elastic rod under quasi-static manipulation," a full length paper, presented at the Workshop on Algorithmic Foundations of Robotics, 2012.

  Z. McCarthy and T. Bretl, "Mechanics and manipulation of planar elastic kinematic chains," a full length paper, presented at the IEEE International Conference on Robotics and Automation, 2012. **Winner of Best Manipulation Paper Award.**

  D. Matthews and T. Bretl, "Experiments in quasi-static manipulation of a planar elastic rod," a full length paper, presented at the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2012. **Finalist for Best Application Paper Award.**

T. Bretl and Z. McCarthy, “Mechanics and Quasi-Static Manipulation of Planar Elastic Kinematic Chains,” to appear in the *IEEE Transactions on Robotics*, 2012.

T. Bretl and Z. McCarthy, “Quasi-Static Manipulation of a Kirchhoff Elastic Rod based on a Geometric Analysis of Equilibrium Configurations,” to appear in the *International Journal of Robotics Research*, 2012.

(Note that these applications of our framework were not within the original scope of our project. Because our results have proven to be transformative, we chose to follow up on this area of opportunity.)

## Project Title: Towards a Science of Securing Network Forwarding

**Project Personnel:** Brighten Godfrey, Matt Caesar, Ahmed Khurshid, and Wenxuan Zhu

### Accomplishments:

We are constructing a system, Veriflow, which automatically verifies security and correctness of computer networks in real time, discovers vulnerabilities, and assists network operators in determining a cause. We have developed a formal model of network behavior, and a set of formal logic algorithms to automatically derive whether the network contains faults. We have developed a prototype implementation and conducted an extensive performance analysis, showing it can verify entire real network topologies with hundreds of devices in less than one millisecond. The University of Illinois Campus Information Technologies and Educational Services (CITES) group has expressed interest in deploying our technology in two of their networks: their campus network, and their Urbana-Champaign Big Broadband (UC2B) network, a community broadband project which is expected to provide gigabit fiber-to-the-premise to 2700 under-served residences and 350 community anchor institutions. We have begun work with CITES on this deployment.

- We completed implementation of our algorithmic extension to handle *packet transformations*, logical operations that manipulate the contents of packet headers (e.g., NAT, label swapping). This improves the generality of our work.
- We continued work with CITES to deploy Veriflow within the University of Illinois network. Our analysis of daily snapshots of network data from CITES uncovered multiple real-world bugs and vulnerabilities, including configuration errors allowing possible denial of service attacks, and bugs in router vendor software.

We have met and exceeded the objectives of our proposal, in particular validating our system's feasibility end-to-end by discovering new real-world vulnerabilities in an operational network.

## Project Title: Enhancing Cyber Security Through Networks Resilient to Targeted Attacks

**Project Personnel:** Yuguo Chen

## Accomplishments:

1. To build statistical models that characterize network resiliency, we fitted the exponential random graph model (ERGM) to the dolphin network which was found to be resilient to targeted attacks. The ERGM is characterized by a list of statistics which are counts of graph structures or features of the network. The local structures we identified that play an important role in the resilience property are geometrically weighted non-edgewise shared partner (GWNSP) and geometrically weighted edgewise shared partner (GWESP), with GWNSP being the most important one.

2. We fitted the exponential random graph model to the dolphin network and estimated the parameters associated with each statistic in the model. The Markov chain Monte Carlo maximum likelihood estimate (MCMCMLE) is obtained by using the R package "ergm." The graphical goodness of fit indicates that our model fits the data well. The random samples generated from the fitted model also show strong resilience to targeted attacks.

3. The ERGM model can help us understand what kind of local features can contribute to the global resilience property. Such a statistical model can also be used to build the Internet and other networks to increase the attack tolerance of those networks. We submitted the paper "Statistical Models for Networks Resilient to Targeted Attacks" which summarizes our findings.

4. We revised the paper on sampling for conditional inference on network data. We studied the asymptotic behavior of the proposed sampling algorithm and showed that the sampling algorithm can still work efficiently for large sparse networks.

5. We built a simple model for spread of infection in a communication network, in which the random attack starts with infection of a randomly selected single node, and then spreads to other nodes due to communication between infected and uninfected nodes. We derived the distribution of extinction time (number of steps needed to infect the whole network) for two special graphs: the loop and the clique. We showed that the clique has the shortest extinction time among the set of networks with the given number of nodes. We conjecture that the chain has the longest extinction time among the set of connected networks, and we are in the process of developing tools to prove this conjecture. We ran the simulation on the Western States Power Grid of the United States, and we also studied the literature on worm propagation in the network.

## Project Title: The Science of Summarizing Systems: Generating Security Properties Using Data Mining and Formal Analysis

**Project Personnel:** Shobha Vasudevan, Parth Sagdeo, and Chen-Hsuan Lin

## Accomplishments:

Benchmarks for demonstrating scalability of PRECIS:

We worked on scaling PRECIS to have advanced features. We tested many large programs on this new scalable version. We tested several UNIX utilities from the SIR repository (sir.unl.edu). This includes bash (the shell), vim (the editor), flex (the lexer), grep (the regular expression parser), and space (an interpreter). This required considerable work to get all the utilities working with PRECIS. PRECIS had to modified considerably. We are able to instrument a much larger set of program constructs. We are also able to evaluate invariants very fast.

Post-deployment debugging and bug localization with PRECIS:

We have developed an extensive debugging framework using PRECIS. We are able to use isolate (post-deployment) buggy runs to specific path predicates. The buggy run statistics are analyzed to determine the likely paths that are erroneous. We are able to do this since PRECIS provides a mapping between assertions, path predicates and multiple paths (multiple concrete paths form an assertion). We are able to localize to very specific regions of the program to detect bugs. Combining statistical analysis with HP Fortify: We are instrumenting predicates in Android apps to gather statistical data, and cluster the relevant program paths. We have also familiarized ourselves with HP Fortify, and are working towards using static analysis from Fortify to guide the clustering inferences.

Exercising program paths using Android's event-based programming model:

We tailored our symbolic execution strategy to Android's event-based programming model as opposed to the traditional sequential model, allowing for more complete analysis of Android apps.

Using bug localization to identify potential hacks in code:

Our PRECIS bug localization framework is intended for post-deployment debugging. We would like to explore if post-deployment security hacks can be used to identify the vulnerable zones in the code using a similar framework. If the vulnerability can be localized to a predicate region in the code, the exact mapping between a failing assertion and the possible parts of the code that have been compromised can be established.

Risks/Areas of Concern

Fortify internal source code is not available, so internal modifications may not be achievable. We will have to write those procedures as post.

## Project Title: A Monitoring Fusion and Response Frameworks to Provide Cyber Resiliency

**Project Personnel:** William Sanders, Brett Feddersen, Atul Bohara, Carmen Cheh, Ahmed Fawaz, Mohamad Noureddine, Uttam Thakore, Benjamin Ujcich

### Accomplishments:

Resilient Architectures – Experience suggests that even heavily defended systems can be breached by attackers given enough time, resources and talent. We propose the concept of a response and recovery engine (RRE) so that a system could "tolerate" an intrusion and provide a base level of service. RRE incorporates modules to monitor current state of a system, detect intrusions, and respond to achieve resilience-specific goals. Our work focuses on a few example attacks. These attacks include lateral movement within a network as part of an Advanced Persistent Threat (APT) and application-level distributed denial of service attacks (DDoS).

Policy-Governed Secure Collaboration – We analyzed the issues surrounding the software-defined networking (SDN) architecture from an accountability standpoint, considering various principals involved (e.g., controller software, network applications, administrators, end users, organizations), mechanisms for assurance about past network state (e.g., data provenance, replicated data stores, roots of trust), thoughts on judging and assessing standards for accountability (e.g., legal, contractual, regulatory), and mechanisms for decentralized enforcement (e.g., blockchain-based smart contracts). We motivated the need for accountability though a network application use case, and we argued that an assured understanding of the past for attribution can help lead to taking better responses for resiliency.

Our RRE work incorporates modules to monitor current state of a system, detect intrusions, and respond to achieve resilience-specific goals. In the area of intrusion detection, we proposed data-driven model-based frameworks to detect abnormal movement in a system. We have used lateral movement within an enterprise network and physical movement within railway transit stations as examples. For the physical movement case, we have developed a framework that uses the building topology and historical user movement data in order to build models that describe normal user movement behavior. During system operation, physical accesses are compared to the models and those that deviate from the model are labeled as malicious. In that work, we use real-world physical data to show that our approach can detect malicious movement in an online manner.

For lateral movement within an enterprise network, we have developed an approach to correlate lateral movement behavior with command and control indicators to identify infected hosts. The approach uses an ensemble of anomaly detectors to have an accurate detection even when attacker deviates from assumed threat model. As an example, we modelled lateral movement within the network using a virus spread model. RRE takes as input information about which host are part of the lateral movement. RRE responds by first allowing the attack to proceed to learn more about it, and then by designing an optimal

response (changing connectivity and healing events) to stop the spread. In this work, we prove that the response results in a stable disease-free equilibrium.

We tackled the problem of ensuring cloud application resiliency against application distributed denial of service attacks (DDoS). We proposed an engine that uses OpenStack's cloud telemetry infrastructure to monitor the cloud applications and uses change point detection to differentiate periods of high load from DDoS attacks. Once an attack has been detected, the engine bootstraps a resiliency response module that use proof of work client puzzles to rate limit attackers in a stateless fashion. Finally, we suggest that the monitoring information can be used to perform horizontal scaling of the cloud application when under attack.

## Project Title: GPS Receiver Integrity Monitoring with Sensor Fusion

Project Personnel: Grace X. Gao

## Accomplishments:

GPS integrity is critical. GPS users need to know not only their positions, but also confidence level of the positions provided by GPS-based navigational devices. Positioning integrity has been well addressed in the Federal Aviation Administration (FAA)-regulated aviation industry for the purpose of guidance and landing of commercial aircraft. The Wide Area Augmentation System (WAAS) to GPS provides Horizontal Protection Level (HPL) and Vertical Protection Level (VPL) in terms of positioning accuracy/integrity for larger aircraft. WAAS focuses on GPS integrity related to GPS satellites and propagation errors. As for characterizing GNSS signal-in-space errors, our prior work [1-3] compares the GPS broadcast ephemerides with the precise ones provided by International GNSS Service (IGS).

1) Many GPS applications require operation in GPS-challenged environments, such as urban area or in a canyon, while larger aircraft fly in open sky. Therefore, GPS receivers are subject to errors and uncertainties caused by the receiver and the environment, such as multipath errors.

2) The accuracy/integrity requirement for navigation in urban and canyon environments is much higher than larger airplanes flying in open sky. Take Boston as an example: the HPL value provided by WAAS with 95% confidence is 28.6 meters, and the VPL value with the same confidence level is 46.7 meters. In Alaska, the numbers are even larger: 49.9 meters and 93.8 meters, respectively for HPL and VPL at Barrow, AK [4]. Such accuracy/integrity is clearly not acceptable for small UAVs in urban environments.

3) Today's GPS users often are equipped with other navigation sensors, such as some combinations of camera vision, Lidar, inertial measurement units (IMUs), etc. In contrast, WAAS provides positioning integrity monitoring for GPS only, not for sensor fusion.

We propose to not only design a system for monitoring positioning integrity, but also to improve integrity. The proposed solution consists of the following elements.

**Task 1:** We will derive and experimentally validate a new algorithm to directly assess and monitor GPS integrity. We propose to use GPS Direct Positioning (DP), instead of traditional scalar tracking as our GPS receiver architecture. DP directly estimates position and velocity by creating a manifold that better represents the probability density function (pdf) of the position and velocity estimates. This manifold can be used directly for bounding the errors and for providing integrity.

**Task 2:** We will derive and experimentally validate an integrity monitoring framework for GPS sensor fusion using camera vision, Lidar and IMU. The framework can be extended to other sensor types. Integrity assessment depends not only on individual sensor error statistical characteristics, but also on how multiple sensors are integrated. We will develop a novel architecture that performs deep sensor fusion on the raw GPS signal level. This new sensor fusion approach also improves navigation integrity.

**Task 3:** We will assess the proposed solutions and aim to achieve the goal of reliable positioning integrity monitoring via safe real-world testing using existing ground vehicle and UAV platforms in PI Gao's group.

# Outreach Activities

To further the goal of broadening the Science of Security Community, we sponsored a conference and two workshops over the lifetime of the funding: 1) Symposium and Bootcamp on the Science of Security (HotSoS 2015), 2) Science of Security for Cyber-Physical Systems Workshop (SoSCYPS 2016), and 3) Workshop on Science of Security through Software-Defined Networking (SoSSDN 2016).

The **2015 Symposium and Bootcamp on the Science of Security (HoTSoS)** was held April 21-22 at the University of Illinois at Urbana-Champaign National Center for Supercomputing Applications. This third annual conference brought together researchers from numerous disciplines seeking a methodical, rigorous scientific approach to identifying and removing cyber threats. As part of the Science of Security program, the HotSoS goal is to understand how computing systems are designed, built, used, and maintained with an understanding of their security issues and challenges. It seeks not only to put scientific rigor into research, but also to identify the scientific value and underpinnings of cybersecurity.

The **Science of Security for Cyber-Physical Systems Workshop (SoSCYPS)** was held on April 11, 2016 in Vienna, Austria as part of CPS Week.

Attacks infiltrating the integrity of vehicular control systems and medical devices have brought to sharp focus the urgency of securing cyber-physical systems. There is a broader discussion about the role of principled security-aware design and analysis in the development of both modern engineering systems such as the Smartgrid as well as in future systems that use advanced AI and machine learning in safety-critical settings. Although there has been a growing interest in these security in the CPSWeek community (increasing number of security related papers in ICCPS, HSCC, RTAS, HyCons), this body of research remains largely disconnected from the mainstream systems security research (USENIX, Oakland, CCS, NDSS). The CPS community has developed analysis and synthesis algorithms, verification tools, notions of observability and controllability, and have been in the forefront of research on emerging applications. The connections between this body of work and systems security research remain unexplored.

The goal of this workshop is to advance the science of security in cyberphysical systems by helping bridge this. We plan to bring together the leaders from these two communities in a full day workshop of invited sessions and panel discussions. Instead of unstructured technical presentations, the speakers and participants will put their research in the context of some broad topics that will help us bridge this gap. Topics of interest will include: Identify hard open problems for academic research in CPS security, data and testbeds in security research amenable to CPS methods, success and fails in designing for resiliency, identify CPS tools and techniques (e.g., verification, synthesis) that can advance systems security research, how to make an impact with CPS security research (where most systems are closed, design cycles are long, and methodologies are slower to change than in cyber systems), and metrics for CPS security.

The program included seven invited speakers and a panel discussion. Each of the invited speakers submitted a paper which will be published as part of the IEEE CPS Week proceedings. Information about the workshop can be found: http://publish.illinois.edu/science-of-security-lablet/science-of-security-for-cyber-physical-systems-workshop/

The two-day **Workshop on Science of Security through Software-Defined Networking** was held on June 16-17, 2016 at the Illinois Institute of Technology in Chicago, Illinois.

Software-defined networking (SDN) is an emerging networking paradigm that promises to convey huge benefits — from reducing the complexities of network traffic control and management to empowering the design of agile networks that can adapt to changing application requirements. The principal feature of SDN is a programmable network operating system achieved through a separation of the control from the data plane. Although there has been a growing interest in innovative uses of SDN to offer fine-grained control and strategies over network-based security functions, this body of research remains largely disconnected from mainstream systems security research. The highly structured approach of SDN offers significant advantages in developing formal guarantees for security. In particular, we may be able to develop a science around the subject that allows us to better measure the effectiveness of any newly developed solutions for security in this space.

The goal of this workshop is to identify opportunities and challenges in using SDNs to advance the 'science of security'. We have brought together leaders from SDN and security in a two-day workshop that consists of invited talks, poster sessions and panel discussions. The speakers and participants will get a chance to place their research in the context of some broad topics that will help explore the area further.

Topics of interest include: SDN principles that support formal and experimental analysis of security, metrics for SDN security, identify hard open problems for academic research in SDN security, SDN-based testbeds and cyber-infrastructures in security research, success and failures in designing for resilient and secure networks, identify tools and techniques that can advance networks/systems security research, how to make an impact with SDN security research.

The program included keynote speakers, Anita Nikolich from the NSF and Frank Acker from the Department of Defense. The program also included 9 invited speakers, a panel discussion and a poster session. More information about the workshop can be found: http://publish.illinois.edu/science-of-security-lablet/workshop-on-science-of-security-through-software-defined-networking/.

# Publications

[1] A. Akce, J. Norton, and T. Bretl, “A brain-machine interface to navigate mobile robots along human-like paths amidst obstacles,” a full-length paper, presented at the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2012.

[2] T. Bretl and Z. McCarthy, “Equilibrium configurations of a Kirchhoff elastic rod under quasi-static manipulation,” a full length paper, presented at the Workshop on Algorithmic Foundations of Robotics, 2012.

[3] T. Bretl and Z. McCarthy, “Mechanics and Quasi-Static Manipulation of Planar Elastic Kinematic Chains,” to appear in the *IEEE Transactions on Robotics*, 2012.

[4] T. Bretl and Z. McCarthy, “Quasi-Static Manipulation of a Kirchhoff Elastic Rod based on a Geometric Analysis of Equilibrium Configurations,” to appear in the *International Journal of Robotics Research*, 2012.

[5] Zhenqi Huang, Sayan Mitra, and Geir Dullerud, “Differentially Private Iterative Synchronous Consensus”, *Workshop on Privacy in the Electronic Society (WPES), collocated with* of 19th ACM Conference on Computer and Communications Security (CCS), Raleigh, NC, 2012.

[6] D. Matthews and T. Bretl, “Experiments in quasi-static manipulation of a planar elastic rod,” a full length paper, presented at the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2012. **Finalist for Best Application Paper Award.**

[7] Z. McCarthy and T. Bretl, “Mechanics and manipulation of planar elastic kinematic chains,” a full length paper, presented at the IEEE International Conference on Robotics and Automation, 2012. **Winner of Best Manipulation Paper Award.**

[8] Quanyan Zhu and Tamer Başar, ``Game-Theoretic Methods for Distributed Management of Energy Resources in the Smart Grid,” Accepted for *8th Annual CMU Electricity Conference*, Pittsburgh, Pennsylvania, March 12-14, 2012.

[9] Xun Gong, Negar Kiyavash, Nabíl Schear, and Nikita Borisov, “Website Detection Using Remote Traffic Analysis”, 12th Privacy Enhancing Technologies Symposium (PETS), Vigo, Spain, July 11–13, 2012, pp. 58–78. Volume 7384 of Lecture Notes in Computer Science.

[10] Ahmed Khurshid, Wenxuan Zhou, Matthew Caesar, P. Brighten Godfrey, “VeriFlow: Verifying Network-Wide Invariants in Real Time,” ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN), August 2012. (Received Best Paper Award). A version of this work was fast-tracked to appear in ACM SIGCOMM Computer Communications Review, October 2012.

[11] Agha, Gul. "Euclidean Model Checking: A Scalable Method for Verifying Quantitative Properties in Probabilistic Systems." (invited talk) *Algebraic Informatics*. Springer Berlin Heidelberg, 2013. 1-3.

[12] N. Aghasadeghi, H. Zhao, L. Hargrove, A. Ames, E. Perreault, and T. Bretl, “Estimation of Impedance Controller Parameters for Biped Locomotion,” a full-length paper, to appear at the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2013.

[13] Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine Meadows, Jose Meseguer, Paliath Narendran, Sonia Santiago and Ralf Sasse. “Asymmetric unification: A new unification paradigm for cryptographic protocol analysis”, in Proc. 24th Intl. Conf. On Automated Deduction (CADE 2013). Springer LNCS, 2013.

[14] M. Johnson, N. Aghasadeghi, and T. Bretl, “Inverse optimal control for deterministic continuous-time nonlinear systems,” a full-length paper, to appear at the IEEE Conference on Decision and Control, 2013.

[15] Young Min Kwon and Gul Agha, “Performance Evaluation of Sensor Networks by Statistical Modeling and Euclidean Model Checking”, 40pp, ACM Transactions on Sensor Networks, Volume 9, Issue 4., 2013.

[16] Ahmed Khurshid, Kelvin Zou, Wenxuan Zhou, Matthew Caesar, P. Brighten Godfrey, “VeriFlow: Verifying Network-Wide Invariants in Real Time,” Symposium on Networked Systems Design and Implementation (NSDI), April 2013.

[17] Peter Dinges, Minas Charalambides, and Gul Agha, “Automated inference of atomic sets for safe concurrent execution”, Technical Report, University of Illinois at Urbana--Champaign, April 2013.

[18] Dennis Griffith and Elsa L. Gunter, “LiquidPi: Inferable Dependent Session Types”, *NASA Formal Methods 2013*, Moffett Field, CA, May 14-16, 2013.

[19] M.H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux. Game theory meets network security and privacy. ACM Computing Survey, 45(3):25:1-25:39, June 2013.

[20] Joseph Sloan, Greg Bronevetsky, and Rakesh Kumar. *" An Algorithmic Approach to Error Localization and Partial Recomputation for Low-Overhead Fault Tolerance on Parallel Systems. "*. In the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks, **DSN,** Budapest, June 2013.

[21] Ahmed Khurshid, Kelvin Zou, Wenxuan Zhou, Matthew Caesar, Brighten Godfrey, “VeriFlow: Verifying Network-Wide Invariants in Real Time,” Open Networking Summit (ONS'13), April 2013. Peter Dinges, Minas Charalambides, and Gul Agha, “Automated inference of atomic sets for safe concurrent execution”, *The 11th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering.* June, 20, 2013.

[22] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, “Resilient Control of Cyber-Physical Systems against Denial-of-Service Attacks,” presented at (and appeared in the Proceedings of) International Symposium on Resilient Control Systems (ISRCS), Resilience Week, San Francisco, Aug. 13-15, 2013.

[23] Gul Agha: “Euclidean Model Checking: A Scalable Method for Verifying Quantitative Properties in Probabilistic Systems” *The Fifth International Conference on Algebraic Informatics, 2013:* LNCS vol. 8080, pp1-3, Springer (invited talk), September 3-6, 2013.

[24] J. Blythe, R. Koppel, and S.W. Smith. “Circumvention of Security: Good Users Do Bad Things.” *IEEE Security and Privacy,* 11(5):80--83, Sept/Oct 2013.

[25] Giang Nguyen, Xun Gong, Anupam Das, and Nikita Borisov. “PnP: Improving Web Browsing Performance over Tor Using Web Resource Prefetch-and-Push.”, poster,*20th ACM Conference on Computer and Communications Security (CCS),* Berlin, Germany, November 4–8, 2013.

[26] Q. Zhu and T. Başar, “Game-theoretic approach to feedback-driven multi-stage moving target defense,” *Proc. GameSec 2013 (Conference on Decision and Game Theory for Security),* November 11-12, 2013; Fort Worth, Texas.

[27] B. Gharesifard, B. Touri, T. Başar, and C. Langbort, “Distributed optimization by myopic strategic interactions and the price of heterogeneity,” accepted for the IEEE Conference on Decision and Control (CDC), Florence, Italy, December 2013.

[28] B. Gharesifard, B. Touri, T. Başar, and C. Langbort, “Distributed optimization by myopic strategic interactions and the price of heterogeneity,” *Proc. IEEE Conference on Decision and Control (CDC)*, Florence, Italy, December 2013, pp. 1174-1179.

[29] Q. Zhu, A. Clark, R. Poovendran, and T. Başar, “Deployment and exploitation of deceptive honeybots in social networks," *Proc. IEEE Conference on Decision and Control (CDC)*, Florence, Italy, December 2013, pp. 212-219.

[30] Gul Agha, “Actors Programming for the Mobile Cloud,” invited talk, *13th International Symposium on Parallel and Distributed Computing*, 8pp, IEEE 2014.

[31] R. Essick, J.-W. Lee, and G.E. Dullerud, “Control of Linear Switched Systems with Receding Horizon Modal Information”, *IEEE Transactions on Automatic Control*, 2014.

[32] Q. Xu, Zhang, C., and G. E. Dullerud, “Stabilization of Markovian Jump Linear Systems with Limited Information”, *American Society Mechanical Engineers Journal of Dynamic Systems, Measurement and Control,* 2014.

[33] Fan Yang, Santiago Escobar, Catherine Meadows, Jose Meseguer, and Paliath Narendran, Theories for Homomorphic Encryption and the Finite Variant Property. Manuscript; February 2014.

[34] P. Cao, K. Chung, A. Slagell, Z Kalbarczyk, R Iyer, “Preemptive Intrusion Detection”, *Symposium and Bootcamp on the Security of Science, (HotSoS ’14)* April 08 - 09 2014, Raleigh, NC, USA, ACM, 2014.

[35] P. Cao, H. Li, A. Slagell, K. Nahrstedt, Z Kalbarczyk, “Personalized Password Guessing,” *Symposium and Bootcamp on the Security of Science, (HotSoS ’14)* April 08 - 09 2014, Raleigh, NC, USA, ACM, 2014.

[36] Santiago Escobar, Catherine Meadows, Jose Meseguer and Sonia Santiago, “A Rewriting- based forward semantics for Maude-NPA”, *Symposium and Bootcamp on the Security of Science, (HotSoS ’14)* April 08 - 09 2014, Raleigh, NC, USA, ACM, 2014.

[37] Zhenqi Huang and Sayan Mitra, “Proofs from Simulations and Modular Annotations”, 17th International Conference on Hybrid Systems: Computation and Control (HSCC 2014), to be held as part of held as part of the seventh Cyber Physical Systems (CPSWeek 2014), April 14-17, 2014, Berlin, Germany.

[38] Zhenqi Huang, Yu Wang, Sayan Mitra, and Geir Dullerud, “On Price of Privacy in Distributed Control Systems”, *3rd ACM International Conference on High Confidence Networked Systems (HiCoNS),* April 15-17, 2014, Berlin, Germany as part of Cyber Physical Systems Week 2014 (CPSWeek 2014).

[39] Buchanan, Craig, Simulation debugging and visualization in the Mobius modeling framework, M.S. Thesis, ECE Dept., Univ. of Illinois, May 2014.

[40] V. Kothari, J. Blythe, S.W. Smith, and R. Koppel. "Agent-Based Modeling of User Circumvention of Security." *ACySE '14: Proceedings of the 1st International Workshop on Agents and CyberSecurity.* ACM. May 2014.

[41] A. Khanafer, T. Başar, and B. Gharesifard, "Stability properties of infected networks with low curing rates," Proceedings of the 2014 American Control Conference (ACC), Portland, Oregon, June 2014, pp. 3591-3596.

[42] A. Gupta, G. Schwartz C. Langbort, S. Sastry, and T. Başar, "A three-stage Colonel Blotto game with applications to cyberphysical security," Proceedings of the 2014 American Control Conference (ACC), Portland, Oregon, June 2014, pp. 3832-3837.

[43] J. Moon and T. Başar, "Control over lossy networks: A dynamic game approach," Proceedings of the 2014 American Control Conference (ACC), Portland, Oregon, June 2014, pp. 5379-5384.

[44] R. Essick, J.-W. Lee, and G.E. Dullerud, "Path-By-Path Output Regulation of Switched Systems with a Receding Horizon of Modal Knowledge", *American Control Conference (ACC)*, June 4-6, 2014.

[45] Gul Agha, "Actors Programming for the Mobile Cloud," invited talk, *IEEE 13th International Symposium on Parallel and Distributed Computing,* 8pp, June 24-27, 2014.

[46] Z. Huang, C. Fan, A. Mereacre, S. Mitra, and M. Kwiatkowska, "Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells", Computer Aided Verification (CAV), July 18-22, 2014.

[47] B. Gharesifard, T. Başar, and A. Dominguez-Garcia, "Designing pricing strategies for coordination of networked distributed energy resources," *Proc. 19th IFAC World Congress (IFAC 2014), Cape Town South Africa, August 25-29, 2014*.

[48] J. Moon and T. Başar, "Minimax control of MIMO systems over multiple TCP-like lossy networks," *Proc. 19th IFAC World Congress (IFAC 2014), Cape Town South Africa, August 25-29, 2014.*

[49] Peter Dinges and Gul Agha, "Targeted test input generation using symbolic-concrete backward execution", *29th IEEE/ACM International Conference on Automated Software Engineering (ASE*). Västerås, Sweden, September 15-19, 2014.

[50] A. Gupta, T. Başar, and G. A. Schwartz, "A Three-Stage Colonel Blotto Game: When to Provide More Information to an Adversary," *Proc. GameSec 2014 (5th International Conference on Decision and Game Theory for Security), November 6-7, 2014; ISI/USC, Los Angeles, California (Springer LNCS 8840, R. Poovendran and W. Saad, Eds)*, pp. 216-233.

[51] Peter Dinges and Gul Agha, "Solving complex path conditions through heuristic search on induced polytopes", *22nd ACM SIGSOFT Symposium on Foundations of Software Engineering*, Hong Kong, November 16-21, 2014.

[52] David M. Nicol and Vikas Mallapura, "Modeling and Analysis of Stepping Stone Attacks", *2014 Winter Simulation Conference*, Savanah, GA, December 7 – 10, 2014.

[53] A. Khanafer, T. Başar, and B. Gharesifard, “Stability properties of infection diffusion dynamics over directed networks,” *Proc. 53rd IEEE Conference on Decision and Control (CDC'14),* December 15-17, 2014; Los Angeles, CA, pp. 6215-6220.

[54] Wang, Yu, Huang, Zhenqi, Mitra, Sayan, and Dullerud, Geir, “Entropy-minimizing Mechanism for Differential Privacy of Discrete-time Linear Feedback Systems”, *Conference on Decision and Control (CDC)*, December 15-17, 2014.

[55] Zhenqi Huang, Sayan Mitra, and Nitin Vaidya, “Differentially Private Distributed Optimization”, *IEEE International Conference on Distributed Computing and Networks (ICDCN)*, January 4-7, 2015.

[56] Q. Zhu and T. Başar, “Game-theoretic methods for robustness, security and resilience of cyber-physical control systems: Games-in-games principle for optimal cross-layer resilient control systems,” *IEEE Control Systems Magazine*, 35(1), February 2015.

[57] P. Cao, K.-W. Chung, A. Slagell, Z. Kalbarczyk, R. Iyer, “Preemptive Intrusion Detection: Theoretical Framework and Real-World Measurements,” *2nd Symposium and Bootcamp on the Science of Security*, HotSoS 2015, April 21-22, 2015.

[58] Minas Charalambides, Peter Dinges, and Gul Agha. “Parameterized, Concurrent Session Types for Multi-Actor Interactions”, Science of Computer Programming, Volumes 115-116, pages 100-126, 1 January – 1 February 2016.

[59] B. Gharesifard, B. Touri, T. Başar, J. Shamma, and C. Langbort, “On the convergence of piecewise linear strategic interaction dynamics on networks,” IEEE Transactions on Automatic Control, Volume 61, Issue 6, June 2016.

[60] Rakesh Kumar. *"On Building Robust Applications by Casting them into Markov Chain Algorithms. "*. In the 47th Annual Asilomar Conference on Signals, Systems, and Computers. November 2013.

[61] Joseph Sloan, Greg Bronevetsky, and Rakesh Kumar. *" An Algorithmic Approach to Error Localization and Partial Recomputation for Low-Overhead Fault Tolerance on Parallel Systems. "*. In the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks, **DSN,** Budapest, June 2013.

[62] B. E. Ujcich, A. Miller, A. Bates, and W. H. Sanders, "Towards an Accountable Software-Defined Networking Architecture", *3rd IEEE Conference on Network Softwarization (NetSoft 2017)*, Bologna, Italy, July 3-7, 2017.

[63] C. Cheh, B. Chen, W. G. Temple, and W. H. Sanders, “Data-Driven Model-Based Detection of Malicious Insiders via Physical Access Logs”, *14th International Conference on Quantitative Evaluation of Systems (QEST 2017),* Berlin, Germany, September 5-7, 2017.

[64] Atul Bohara, Mohammad A. Noureddine, Ahmed Fawaz, William H. Sanders, “An Unsupervised Multi-Detector Approach for Identifying Malicious Lateral Movement”, *36th IEEE International Symposium on Reliable Distributed Systems (SRDS 2017)*, Hong Kong, September 26-29, 2017.