# Modeling and Verifying Intelligent Automotive Cyber-Physical Systems*

Sumit Kumar Jha Gita Sukthankar
EECS Department, University of Central Florida, Orlando, USA
jha,gitars@eecs.ucf.edu

**Abstract**

Exhaustive state space exploration based verification of cyber-physical system designs remains a challenge despite five decades of active research into formal verification. On the other hand, models of intelligent automotive cyber-physical systems continue to grow in complexity. The testing of intelligent automotive models often uses human subjects, is expensive, and can not be performed unless the system has already been prototyped and is ready for human interaction. We propose the use of machine learning methods to learn stochastic models of human-vehicle interaction. Simulation based validation of even critical designs often uses randomized testing and is subject to financial budget considerations in practice. We argue that a combination of statistical and randomized verification approaches are suitable for verifying complex intelligent cyber-physical systems in an era of multi-core processors.

## 1 Introduction

Cyber-physical systems, specially intelligent automobile applications, interact closely with our daily life. Given the critical nature of the designs and the limited resources available for their validation, a key goal is to develop automated verification techniques that are scalable to the complex nature of cyber-physical systems. The involvement of the human user in the behavior of these intelligent cyber-physical systems makes the challenge of validating them even more difficult. In this paper, we identify directions for future research that may enable the verification of intelligent automobile cyber-physical systems.

## 2 Research Agenda

### 2.1 Closing the Loop: Building Models of Human Behavior

Sanity checks in software implementations of cyber-physical systems (like buffer overflow, thread priority inversion) have received considerable attention from researchers over the last three decades. However, the validation of behavioral properties that establish the correctness or safety of intelligent automobile cyber-physical systems needs to model the human user and her interactions with the intelligent systems on-board. While the importance of field tests with human subjects cannot be overemphasized, these tests are (i) expensive, (ii) require a complete prototype implementation, and (iii) need to be repeated as newer models of intelligent systems are built. We propose (machine) learning the behavior of human subject interacting with an intelligent automobile cyber-physical system. Our approach relies on obtaining time series data from sensors reporting on automobile state and human reaction (steering, brakes, gas, facial images) to record the behavior of individuals involved in testing of prototyped cyber-physical systems.

The problem of modeling human behavior has been studied extensively toward the goal of recognizing and classifying human behavior. Although many of the models are discriminative

*The first author acknowledges the support of faculty start-up funds from the University of Central Florida. The second author acknowledges the support of NSF Career Award IIS-0845159.

(e.g., conditional random fields), models based on learning conditional probability distributions can function as a generative models of human behavior; parameters for these models can easily be learned using standard methods such as expectation-maximization. However, less attention has been devoted to determining the structure of the models and very little to principled techniques for determining the representation of the model beyond relying on the researcher's intuitions of the domain.

We propose to exploit existing psychological theories of human behavior to improve accuracy of modeling by basing our state representation and action selection on validated models. By shifting to a problem representation based on psychological theory rather than hand-coded models, we have demonstrated that it is possible to simultaneously improve modeling performance and generalize our models to related tasks without the added complexity of trying to learn a model from data. Moreover, we believe that this will lead to models that generalize better across cognitively-related problems.

Humans create *mental models*, internal explanations in their thought processes for how things work in the real world, when they reason about their environment; eliciting the content and structure of these internal mental models is an important part of cognitive psychology. In addition to general cognitive theory on internal human representations, psychologists have developed very specific theories to model lower-level skills, such as visually-guided steering, to address issues such as route selection, obstacle avoidance, and the interception of moving objects. For instance, given a set of obstacles, humans rarely function as an optimal route planner, selecting the shortest path to their goal. We have demonstrated an approach for path prediction based on a model of visually-guided steering that has been validated on human obstacle avoidance data and trained in simulation. By basing our path prediction model on egocentric features that are known to affect human steering preferences, we can improve on strictly geometric models [1, 2].

### 2.2 When to Stop Simulation Based Verification?

**Statistical Trade-off between Cost of Simulation and Possible Loss from Erroneous Designs:** We seek to quantify the trade-off between the budget for testing and the potential financial loss from an incorrectly designed intelligent cyber-physical system. We have developed an algorithm [4] that minimizes the overall cost of using an intelligent cyber-physical system: we perform random sampling based testing of the system unless the cost of performing an additional simulation exceeds the possible expected loss from using an incorrectly designed intelligent cyber-physical system. We have demonstrated that our algorithm needs only a logarithmic number of test samples in the cost of the potential loss from an incorrect validation result. We also show that our approach remains sound when only upper bounds on the potential loss and lower bounds on the cost of simulation are available.

In order to expedite the validation of models of intelligent cyber-physical systems, we seek to extend these approaches from randomized testing to a combination of more systematic testing and the use of non-i.i.d. (independent and identically distributed) samples. While it is easier to prove statistical bounds on approaches that use random sampling, it is more meaningful to analyze rare behaviors of such models and prove safety results using samples that are not necessarily random.

### 2.3 Randomized Verification of Intelligent Automobile CPS

Our current technique [3] extends earlier work on using *Iterative Relaxation Abstraction* (IRA) to prove the correctness of linear hybrid automata and the use of *Counterexample Guided Abstraction Refinement* (CEGAR) for analyzing models of cyber-physical systems. In our approach, several *low dimensional over-approximate relaxation abstractions* of the original linear hybrid automata are constructed in a distributed manner. Each low dimensional relaxation abstraction is then analyzed by a traditional model checking algorithm to determine if there are any counterexamples in the low dimension abstraction. Correctness of the low dimensional abstractions is then used to argue the correctness of the overall high dimensional system.

The verification of critical high assurance components of intelligent automobile cyber-physical

systems in an era of multi-core processors will require the use of verification methods that can be easily distributed. Traditional distributed approaches to formal verification have not scaled enough to be of immediate use in verifying intelligent automotive cyber-physical systems. Because of the daunting complexity of the intelligent automobile CPS designs and the breakdown of Moore's law for single core processors, it is important to develop distributed methods for validating such complex models. We believe that distributed verification of low dimensional abstractions may be a solution to the problem.

## 3 Challenge Problems, Community and Milestones

Challenge problems for verification of cyber-physical systems need to be made available to the general community. The website data.gov allows for free hosting of models. Several classes of models need to be available: (i) Software (ii) Models (like, Simulink) (iii) Equation/Vehicle Dynamics Models. These models need to be annotated and the validation criterion for these models should be available. Time-series data from human interactions with such models need to be made available to researchers.

In order to facilitate rapid progress and identify winning directions, an annual competition for verifying or finding bugs in intelligent cyber-physical systems should be held. The SMT community and the hardware verification community have been very successful in making rapid strides using an annual competition to benchmark tools. Community building efforts in this area should draw from the expertise of researchers throughout the world. In that context, it is important to host a virtual workspace for collaborators to express interest and get together. A website (like those hosted by GSRC in the semiconductor validation space) will be essential. Further, a workshop that brings together the designers of automobile applications and validation researchers together would be helpful.

## References


[1] B. Tastan and G. Sukthankar. *Exploiting human steering models for path prediction.* In Proceedings of the International Conference on Information Fusion, pp. 1722-1729, 2009.

[2] B. Tastan and G. Sukthankar. *Leveraging Human Behavior Models to Predict Paths in Indoor Environments*, Submitted Aug 2010.

[3] S. K. Jha, *d-IRA: A distributed reachability algorithm for analysis of linear hybrid automata*, in International Conference on Hybrid Systems Computation and Control, April 2008.

[4] S. K. Jha, C. J. Langmead, S. Ramesh, S. Mohalik *When to Stop Verification? Statistical Trade-off between Cost of Simulation and Possible Loss from Erroneous Designs*, Submitted September 2010.


## 4 Biography

Dr. Jha is an Assistant Professor with the Computer Science Department at the University of Central Florida, Orlando. He received his Ph.D. in Computer Science at Carnegie Mellon University, where he worked on developing algorithms for validation and synthesis of complex stochastic systems using high level behavioral specifications. Dr. Jha has also worked on more traditional formal validation and machine learning problems at Microsoft Research, General Motors and INRIA, France.

Dr. Gita Sukthankar is an assistant professor in the School of Electrical Engineering and Computer Science at the University of Central Florida, and an affiliate faculty member at UCF's Institute for Simulation and Training. She received her Ph.D. from the Robotics Institute at Carnegie Mellon, an M.S. in Robotics, and an A.B. in psychology from Princeton University. From 2000–2003, she worked as a researcher at Compaq Research/HP Labs (CRL) in the handheld computing group. In 2009, Dr. Sukthankar was selected for an Air Force Young Investigator award, the DARPA Computer Science Study Panel, and an NSF CAREER award. Her research focuses on social models within RAP systems (Robots, Agents, and People), with a particular emphasis on studying the behavior of people within games and simulation environments where people and agents can interact on an "equal footing".