Call for Papers

Journal of Defense Modeling and Simulation: Applications, Methodology, Technology (JDMS)

Special Issue: Modeling & Simulation for Cyber Security of Autonomous Vehicle Systems

Guest Editors

Dariusz Mikulski, U.S. Army TARDEC   Greg Hudas, U.S. Army TARDEC

Sajal K. Das, Missouri Univ. Science and Technology   F.L. Lewis, Univ. Texas Arlington

Introduction

Recent advances in autonomous cyber-physical systems show promise for improved reconnaissance, surveillance, and security in foreign and domestic conflicts. However, cyber-physical systems also present new and unevaluated sets of attack surfaces in communications and controls. As such, the modeling and simulation of cyber security in autonomous systems is a critical research area that will ultimately dictate the ways these systems should interact with people and each other. Thus, the goal of this Special Issue is collect a comprehensives body of descriptive and prescriptive approaches to modeling and simulating cyber security threats, defense techniques, and overall frameworks in highly dynamic and hostile environments. Potential contributions can include, but are not limited to:

- General frameworks for modeling and simulation test-beds that result in advanced development of components of a cyber security system evaluation
- Case studies of known autonomous vehicle attack surfaces at the respective layers of the Open System Interconnection (OSI) hierarchy
- Autonomous vehicle threat quantification: tools, techniques, and methods
- Definition of risk for autonomous vehicle cyber security
- Use of existing standards (e.g., NIST, ISO) for autonomous vehicle cyber security modeling
- Training for critical incident response in cyber security
- Use of legacy cyber attack data to prescribe different threat types (e.g. scenario planning)
- Intelligent software decoys (e.g., Honey Nets) and other techniques that result in autonomous vehicle rapid maneuvering that adapt to the threat

Papers submitted should not be concurrently under review at another conference, journal, or similar venue.

Instructions for Manuscript Preparation

For manuscript formatting and other guidelines, please visit the Author Guidelines for JDMS.

Note: Manuscripts must not have been previously published or be submitted for publication elsewhere. Each submitted manuscript must include title, names, authors' affiliations, postal and

e-mail addresses, and a list of keywords. For multiple author submission, please identify the corresponding author.

Due Dates

May, 2015	Manuscripts Due
June 2015	First Review Decisions
July, 2015	Revised Manuscripts Due
September, 2015	Final Decisions
Winter 2016	expected date of publication

Submissions for full paper review

All manuscripts must be submitted electronically through the paper submission system to the JDMS Manuscript Submission System. In the title page, author(s) must specifically mark that the paper is intended for this special issue as follows: "Submission for the Special Issue of JDMS: **Modeling & Simulation for Cyber Security of Autonomous Vehicle Systems**. Please follow the guidelines for submission on the Manuscript Central site.

Final paper submissions

Each final submission must be prepared based on the JDMS journal requirements (see the Author Guidelines for JDMS page).

Guest Editors:

- Dariusz Mikulski
  U.S. Army, Ground Vehicle Robotics, TARDEC Warren, MI
  dariusz.mikulski@us.army.mil

- Greg Hudas
  U.S. Army, Ground Vehicle Robotics, TARDEC, Warren, MI
  greg.hudas@us.army.mil

- Frank Lewis
  Univ. of Texas at Arlington, Dept. of EE, Arlington, TX
  lewis@uta.edu

- Sajal Das
  Missouri Univ. of Science and Technology, Dept. of Computer Science, Rolla, MO
  sdas@mst.edu

For questions contact:

Vicki Pate, Managing Editor
Journal of Defense Modeling & Simulation
vmpate@scs.org

Frank Lewis, Guest Editor
lewis@uta.edu