

Call for Papers

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

Special Issue: Modeling and Simulation to Support Cyber Defense (J17-3)

Introduction

Complex environments, such as the cyber domain, can benefit from modeling and simulation to understand the impact of new concepts and capabilities to cyber defense. In addition, recent improvements in modeling & simulation techniques, especially in cyber range based experimentation, testing & evaluation, have the potential to enable the next generation of cyber defense approaches to enterprise computing systems and cyber-physical systems. We are, therefore, looking for modeling and simulation papers for defense of enterprise or cyber-physical systems in the following areas.

- Description, and use of novel analytical modeling approaches such as probabilistic, game-theoretic, and ontological for experimentation, situational awareness, analysis, or decision making.
- Description and use of live, constructive, or virtual models at varying levels of fidelity using modeling and simulation paradigms, including System Dynamics, DEVS, and Agent-based.
- Approaches for modeling of cyber and physical dependencies and defenses of systems and processes.
- Interoperability of models and model validation.
- Uses of simulation of cyber defense of autonomous systems: design, tools, techniques, and methods.
- Analysis of efficacy of autonomous cyber defenses of enterprise and cyber-physical systems.
- Mission risk analysis, impact analysis of attacks and defenses, strategies and policies for defense, and unintended consequences.
- Use of cyber-attack data to identify different threat types, adversary tactics, pre-attack signatures.
- Use of cyber data in novel model instantiation or validation scenarios.
- Analysis of human factors.
- Novel instrumentation, tools, platforms, or applications to support planning, deployment, execution, and analysis of experiments.
- Modeling and risk assessment of a cybersecurity environment with malware activities, online sensor measurements, and adversary tactics.

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

Submission of papers January 30, 2018
Expected date of publication Fall 2018

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 and Simulation to Support Cyber Defense.**" 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:

Dr. Suresh K. Damodaran¹, MITRE
Mr. Jackson Ludwig, MITRE
Dr. Neal Wagner, MIT Lincoln Laboratory
Dr. Michael L. Winterrose, MIT Lincoln Laboratory
Dr. Hasan Cam, ARL, US Army

For questions contact:

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

Suresh Damodaran, PhD, Guest Editor
sdamodaran@mitre.org

¹ **The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.**