The 15th IEEE International Conference on Machine Learning and Applications (IEEE ICMLA'16), Anaheim, USA
18-20 December 2016
www.icmla-conference.org/icmla16

Workshop on
Machine Learning in Security of Cyber-Physical Systems (MLSCPS)

AIMS AND SCOPE

In recent years, security of cyber-physical systems (CPS, physical systems controlled by computer-based algorithms) has been an important challenge for many researchers. Despite recent advancements in the area of cyber-security, there are still numerous reports on cyber-attacks. Security of CPS plays an important role in assuring successful performance of industrial and critical infrastructures such as power systems, transportation systems, and smart medical systems.

A major cyber-attack on the U.S. electrical grid could result in economic losses in the trillions of dollars. Studies have demonstrated that smart grids are vulnerable to security threats at both the physical and logical levels. Threats to the physical layer include theft, vandalism, and sabotage, while protecting the logical layer means protecting data. The smart energy sector has been subjected to a wide spectrum of attacks over the last five years. Web-based applications and supervisory control and data acquisition (SCADA) systems are vulnerable to entities intruding between data and the data-gathering systems.

Security of current and future biomedical devices together with their connectivities to smart medical platforms will be of major concern to public health in the future. Recently for example, the U.S. Department of Homeland Security underscored some threats affecting almost three hundred medical devices. There is additional concern about security in transportation systems. New advances in transportation systems, including connected/autonomous vehicles and unmanned aerial vehicles, increase the attack surface of transportation systems and make them more vulnerable to cyber-security attacks.

MLSCPS will serve as special session for reporting advances in all aspects of machine learning in security of cyber-physical systems, including theory, tools, applications, systems, testbeds, and field deployments. Improvements in Machine Learning (ML) provide new solutions and challenges to the security of cyber-physical systems used in power, medical and transportation systems.

The goal of this session is to bring together professionals, researchers, and practitioners in the area of cyber security to present, discuss, and share the latest findings in the field, and exchange ideas that address real-world problems with real-world solutions.

The special session opens to everybody as well as industrial partners to make contribution in this area. Topics for this session include, but are not limited to:

- Security of networked control systems, applications in power, transportation, and bio-medical systems
- Intrusion detection techniques

- Secure communication protocols for cyber-physical systems
- Security risk analysis, modelling, evaluation, and management
- Software and hardware security
- Cloud and mobile Security
- Attack and threat models
- Techniques to detect and overcome new type of attacks
- Security of smart grid systems
- Network and sensor security
- Estimation theory
- Pattern recognition
- Security of autonomous vehicles and unmanned aerial vehicles
- Industrial Control Systems

Papers should be submitted for this special session at the regular paper submission website (http://www.icmla-conference.org/icmla16/). Papers should not exceed a maximum of 6 pages (including abstract, body, tables, figures, and references), and should be submitted as a pdf in 2-column IEEE format. Detailed instructions for submitting the papers are provided on the conference at home page.

Special Session Chair

Dr. Arman Sargolzaei
Florida International University, USA

Program Committee Members:

Dr. Ben Amaba	IBM, USA
Dr. Jeff Daniels	Lockheed Martin Co, USA
Dr. Kang Yen	Florida International University, USA
Dr. Mohammad Al-Faruque	University of California-Irvine, USA
Dr. Arif Sarwat	Florida International University, USA
Dr. Saman Sargolzaei	Rancs Group LLC, USA
Dr. Mohamed Abdelghani	University of Alberta, Canada
Alireza Abbaspour	Florida International University, USA
Shirin Noei	Florida International University, USA

Important Dates:

Paper Submission Deadline	**August 6th, 2016**
Notification of Acceptance	**September 7th, 2016**
Camera-Read Papers	**October 1st, 2016**

If you have any question about this session, please do not hesitate to ask your question to a.sargolzaei@gmail.com