GameSec 2025, Athens Greece
Tutorial on Game theory and Artificial Intelligence Methods for Security and Trust
Monday, October 13, 2025
Organizer: John S. Baras
Co-Chairs: John S. Baras and Tansu Alpcan

Program

9:00am - 9:30 am
Introduction and Goals of the Tutorial
John S. Baras
University of Maryland College Park, USA, and Archimedes AI Research Center, Greece
baras@umd.edu

9:30am – 10:30am
An Introduction to Game-Theoretic Framework for Multi-Agent Decision-Making with Applications to Security
Tamer Başar
University of Illinois Urbana-Champaign, USA
basar1@illinois.edu

Abstract
With its rich set of conceptual, analytical, and algorithmic tools, *game theory* has emerged as providing a versatile and effective framework for addressing issues of resilience, reliability and security in networked systems. This tutorial will introduce the key elements of this modeling paradigm and discuss various game-theoretic solution concepts of direct relevance to non-cooperative decision-making. The talk will also cover derivations of these (equilibrium) solutions as well as iterative schemes for their computation. It will conclude with some specific examples of security games within the context of cyber-physical systems.
10:30am – 11:00am
Coffee Break

11:00am – 12:00pm
Reward Schemes and Incentives in Proof of Stake Blockchain Protocols
Vangelis Markakis
Athens University of Economics and Business and Archimedes AI Research Center, Greece
markakis@gmail.com

Abstract
This talk focuses on game-theoretic aspects that arise in the design of reward schemes in blockchain protocols. The first part concerns a model for pool formation in Proof of Stake protocols. In such systems, stakeholders can form pools as a means of obtaining regular rewards from participation in ledger maintenance and block production, with the power of each pool being dependent on its collective stake. The question of interest here is the design of reward schemes that suitably split earned profits among pool members. With this in mind, we initiate a study of the well-known Shapley value scheme into the context of blockchains. We provide comparisons

between the Shapley mechanism and the more standard proportional scheme, in terms of attained decentralization (i.e., number of pools formed at equilibrium), and in terms of susceptibility to Sybil attacks, i.e., the strategic splitting of a players' stake with the intention of participating in multiple pools for increased profit. The second part of the talk is motivated by a different application scenario and investigates the impact of reward schemes on blockchain governance. We introduce a model of elections where there is a ground truth (i.e., a ``correct'' outcome), and where stakeholders can only choose to delegate their voting power to a set of delegation representatives (DReps). As a way to motivate the representatives to exert effort and discover the ground truth, a reward scheme can be used based on the total delegated stake attracted by each DRep. We analyze different schemes in this context with respect to their equilibrium properties, given an available monetary budget. Our findings provide insights into the design of effective reward mechanisms and optimal committee structures (i.e., how many DReps are enough) in such systems with the goal of maximizing the probability for selecting the correct outcome.

12:00pm – 13:00pm

Posted Price Mechanisms for Combinatorial and Procurement Auctions

Dimitris Fotakis
National Technical University of Athens and Archimedes AI Research center, Greece
fotakis@cs.ntua.gr

Abstract
In algorithmic mechanism design, we aim to allocate goods to self-interested agents in a way that guarantees dominant-strategy incentive compatibility (a.k.a. truthfulness), social efficiency (at least approximately) and computational efficiency. After a brief introduction to algorithmic mechanism design, we will focus on the design of posted price mechanisms, where the agents arrive online and are offered take-it-or-leave-it prices, for combinatorial auctions and procurement auctions. Posted price mechanisms are particularly appealing due to their simplicity, obvious truthfulness and explainability of the resulting allocation. We will first discuss posted price mechanisms for combinatorial auctions when the agents arrive in random order. Next, we present the prophet inequality, its extensions and its applications to posted price mechanisms in the Bayesian setting, where the agent valuations are drawn as independent samples from known distributions. We will conclude with the main idea behind a posted price competitive mechanism for procurement auctions with submodular values.

13:00pm – 14:00pm

Lunch

14:00pm – 15:00pm

An Introduction to ML and AI methods for Networked Systems Security and Trust

John S. Baras
University of Maryland College Park, USA, and Archimedes Research Center, Greece

Abstract
Machine Learning (ML) and Artificial Intelligence have emerged as important new technologies that can facilitate and accelerate substantially research, development and practical usable

methodologies and algorithms, in many areas of critical importance to society, economy, work, healthcare, engineering, manufacturing. This tutorial will introduce key and recent elements of ML, Reinforcement Learning (RL) and AI. The application area of focus is security and trust in several networked systems domains. Will review earlier work with practical applications to the security of routing protocols for mobile adhoc networks (MANETs). Will then introduce a rigorous foundation of AI emphasizing the need to integrate ML with Knowledge Representation and Reasoning (KRR). Will review the two main approaches for KRR, namely Semantic Vector Spaces (on which Transformers and Large Language Models (LLM) are founded) and Knowledge Graphs (KG) (which provide efficient methodologies and models for capturing and compacting knowledge). Next will describe results and open problems on the integration of LLMs and KGs towards efficient KRR systems. Will next describe results and open problems on the integration of ML, RL and KRR towards AI assistants, including agentic AI systems. We will describe how these novel and emerging approaches hold promise to efficient integrate domain (expert) knowledge with data driven information. We will describe some recent results on using these methods and resulting constructs to develop efficient and high-performance AI assistants in medical diagnosis and security and trust. We will close with a discussion of the complementary relationship between game theoretic methods and AI methods for security and trust, including the recently emerged topic of security and trust games between teams of AI agents.

15:00am – 15:30am
Coffee Break

15:30pm – 16:30pm
Constraints-Enforcing RL Solutions for Ensuring Safety and Security
Elena Stai
National Technical University of Athens, Greece
estai@mail.ntua.gr

Abstract
This tutorial explores AI-driven methods for tackling optimization problems with long-term objectives and lookahead constraints. Model Predictive Control (MPC) has long been the standard approach for such problems, but it often entails high computational cost and depends heavily on the availability of accurate forecasts. Reinforcement Learning (RL) offers a compelling alternative; however, conventional RL methods typically fall short in ensuring constraint satisfaction. We will review recent advances in Safe and Constrained RL, addressing both training/offline and deployment/online phases. These problems are commonly formulated as Constrained Markov Decision Processes (CMDPs). A typical strategy to enforce constraints is to assign large negative rewards to violating states. Alternatively, RL can be combined with Lagrange optimization, where constraint violations are penalized using dynamically adjusted Lagrange multipliers. A further promising direction lies in hybrid methods that integrate RL and MPC, embedding RL-based value functions into MPC cost formulations to overcome the limitations of both paradigms. Finally, we will showcase applications of these methods to the optimal control of energy storage systems in power grids, enabling their safe and secure operation under increasing shares of renewable energy and the growing demands of electromobility.

16:30pm – 17:30pm
Resilient AI for Cyber Physical Systems
Panagiotis Papadimitratos
Royal Institute of Technology (KTH), Sweden
papadim@kth.se

Abstract
Artificial intelligence (AI) is becoming a key element for cyber-physical systems (CPS), be it autonomous vehicles or emerging communication infrastructures. Nonetheless, the integration of AI introduces vulnerabilities: adversarial inputs, poisoned data, and sensor spoofing can undermine safety and reliability. This tutorial talk explores how to design resilient AI for CPS. We consider threat models and defense strategies, driving the presentation based on case studies; we will refer to recent work, e.g., road condition classification based on federated learning, misbehavior detection in vehicular platoons, GNSS spoofing detection, and lightweight edge AI for wireless systems, as time permits.

17:30pm - 18:30pm
Open Panel Discussion and Q&A with Lecturers
Moderator: Tansu Alpcan
University of Melbourne, Australia
tansu.alpcan@unimeb.edu.au