GW | SEAS

Cyber Security and Privacy Research Institute (CSPRI)

presents

Adversarial Machine Learning and Wireless Security for 5G and Beyond

Speakers

Dr. Yalin Sagduyu, Director & Dr. Tugba Erpek, Lead Scientist
Networks and Security Division, Intelligent Automation, Inc. (IAI)

Thursday, November 19, 2020 at 12:00 noon

This event will be held as a webinar through WebEx.

Please RSVP at Eventbrite (https://bit.ly/2K0uaE4) to register for the talk.
Registrants will receive the WebEx video conference details from Dr. Hurriyet Ok.

Abstract

Machine learning provides automated means to capture complex dynamics of wireless spectrum and support better understanding of spectrum resources and their efficient utilization. Empowered by recent advances in algorithmic and computational capabilities, deep learning has emerged as a viable solution to solve complex tasks involved in wireless communication systems including 5G and beyond. As deep learning has become a key component in wireless communication systems, a new attack surface arises due to adversarial machine learning that targets the learning process embedded in wireless communications. In this talk, we will first introduce the basics of adversarial machine learning using examples from different data domains such as computer vision and natural language processing. Then, we will discuss the extension of adversarial machine learning to the wireless domain and feature the unique characteristics of wireless medium that make wireless communications susceptible to a broad range of new security threats. Specifically, we will take a deep dive into deep learning applications in 5G and beyond, and present how next-generation communication systems are becoming vulnerable to the new attack surfaces supported by adversarial machine learning. We will discuss these new security threats for 5G and beyond with examples from spectrum sharing, signal classification, user authentication, and network slicing.

Biographies

Dr. Yalin Sagduyu is the Director of Networks and Security Division at Intelligent Automation, Inc. (IAI). He received his Ph.D. degree in Electrical and Computer Engineering from University of Maryland, College Park. At IAI, he directs a division of over 50 research scientists and engineers and executes a broad portfolio of R&D projects on wireless communications, network security, and machine learning.

Dr. Tugba Erpek is a Lead Scientist at Networks and Security Division at IAI and Adjunct Research Professor at the Hume Center at Virginia Tech. She received her Ph.D. degree in Electrical and Computer Engineering from Virginia Tech. Her R&D work covers wireless communications, physical layer security, machine learning, network protocol design and implementation, and resource allocation.

The intent of this and future Cyber Security and Privacy Research Institute (CSPRI) webinars is to give GW faculty and students glimpses of the vibrant security and privacy private sector in the Washington region and to promote dialog and debate regarding breakthrough initiatives. The potential for support for research or conference papers on related topics will be part of the discussion.