Providing Security for Edge Devices in Last Mile Connection

Hong Zhao, Professor of Electrical and Computer Engineering
Fairleigh Dickinson University

******** Event is dedicated for Celebrating the IEEE Day 2023 ********

Sponsor by IEEE Computer NY Chapter, IEEE Systems, Man, and Cybernetics (SMC) NY Chapter, IEEE Communications NY Chapter, IEEE Student Branch at LIU-Brooklyn, NY, IEEE Student Branch at NYU, IEEE Student Branch at CityTech, CUNY

October 3, Tuesday, 6~ 8:00 PM
Virtual Seminar through IEEE WebEx hosting
For program questions, Please email to ptchung@ieee.org or xinzhou.wei10@citytech.cuny.edu

Join WebEx meeting

https://ieeemeetings.webex.com/ieeemeetings/j.php?MTID=m89d3cd02c1f010d41961563c6e4a6994

Meeting number: 2533 148 8183
Meeting password: nPkPReAt292

- Event Agenda -

***Event Agenda:* 6:00 PM**
Welcome Remark – IEEE NY Section Chair, Robert M. Pellegrino
6:10 ~ 7:10 PM (Presentation)

Providing Security for Edge Devices in Last Mile Connection

Hong Zhao, Professor of Electrical and Computer Engineering
Fairleigh Dickinson University

7:10 PM Q/A The event is free to attend.
ALL ARE WELCOME

Abstract: Communication security is one of the top security challenges for connected devices, especially for physical devices connected through wireless access networks. Wireless links, often as the last mile, use un-guided medium as communication channels, and therefore gathering wireless data transmission is easier when compared to traditional cable systems. Wireless communication is thus prone to security vulnerabilities from the very beginning. At the same time, parts of device hardware are designed for use by everyone, which gives potential attackers physical access to the system. Most current wireless access networks apply conventional cryptographic approaches implemented on upper-layer operations to provide confidentiality/authentication/data integrity. This generally requires a high computational platform and managing secrets, which may not exist in all IoT devices. In this talk, physical layer security is addressed at waveform level by applying chaos theory. The cost-effective features include the simplicity of communication setup, the low power-consuming devices to generate and control chaotic signals, and no need of using complicated and energy consuming devices to avoid nonlinearities. The sensitivity to initial condition and complex dynamic feature make it a promising approach for physical layer security.

Biography: Hong Zhao received a Ph. D from New Jersey Institute of Technology in Electrical and Computer Engineering. She is a tenured Professor of Electrical and Computer Engineering at Fairleigh Dickinson University, New Jersey, US. Her research focuses on various aspects of broadband communications and computer security including Network Traffic/Performance/Security Analysis and Modeling, and Hardware Security and Trust. Dr. Zhao serves as Associate Editor of the Journal on *Multidimensional Systems and Signal Processing*, and Editor of the *Journal of Computing and Information Technology*. She has been a TPC chair of WTS 2019 and board chair of the WOCC (2017-2018). Professor Zhao also serves as Chair of the IEEE North Jersey Section (2023-2024). Dr. Zhao received Visiting Faculty Research Program (VFRP)

Awards from the United States Air Force Research Lab (AFRL) in 2014-2016, Summer Faculty Fellowship Program (SFFP) Awards from the Air Force Office of Scientific Research (AFOSR) in 2017-2021, and 2015 IEEE Region 1 award for Outstanding Support for the Mission of the IEEE, MGA, REGION 1 and Section. She is a recipient of the National Research Council (NRC) fellowship award in 2022.