IEEE
COMMUNICATIONS
SOCIETY

AI and ML in Security Special Interest Group

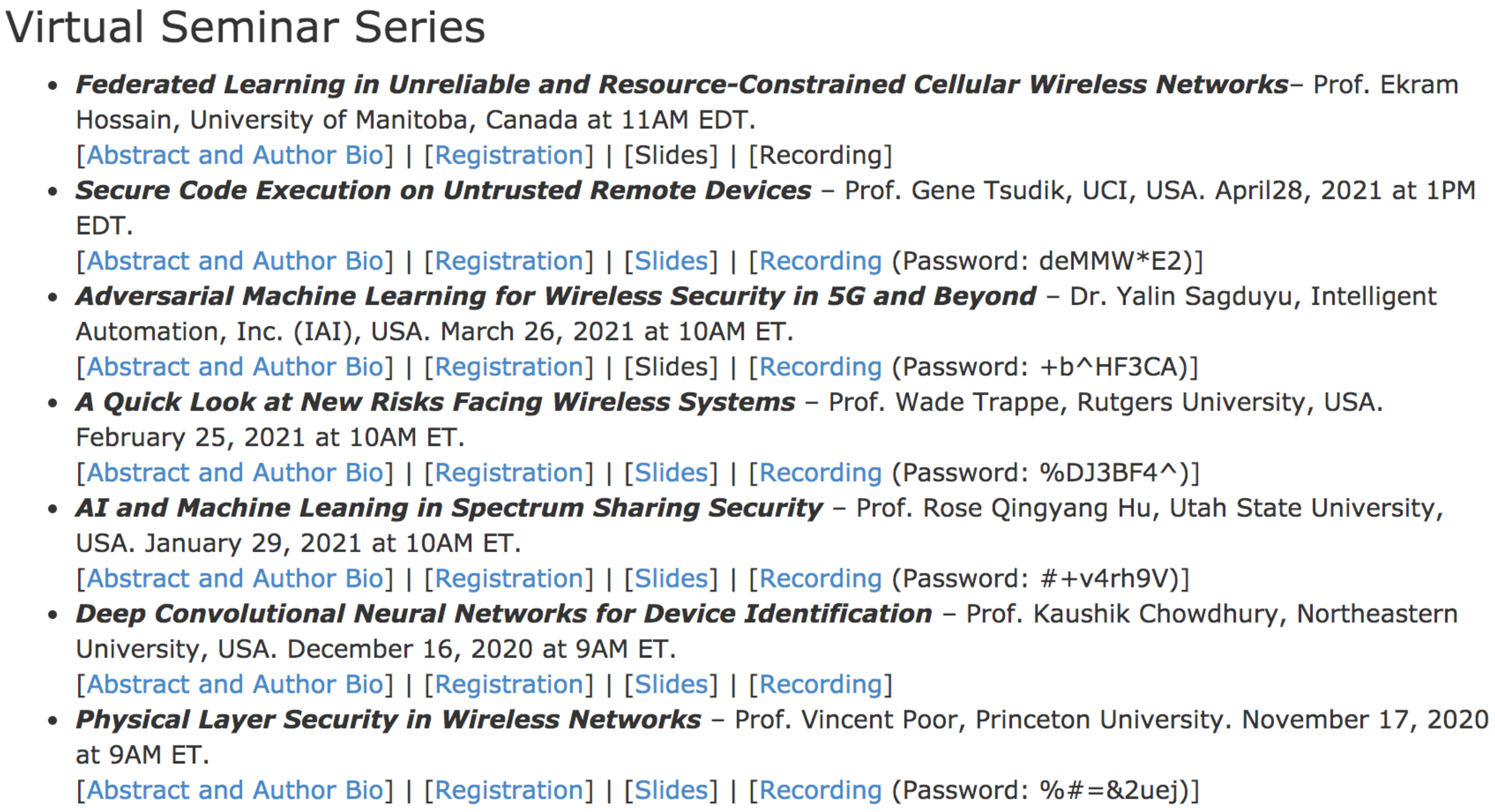
Chair: Prof. K.P. (Suba) Subbalakshmi,
Fellow National Academy of Inventors
http://www.kpsuba.com
Stevens Institute of Technology,
ksubbala@stevens.edu;
Jefferson Science Fellow

Vice Chair:
Prof. Dola Saha, University at Albany, SUNY

Introduction to the AIMLSec-IG

- Currently 325 members in LinkedIn
- To join Sec-IG, use the LinkedIn group:
  - http://www.linkedin.com/groups?home=&gid=5070076&trk=anet_ug_hm
  - The group is also searchable under the name of IEEE Special Interest Group on AI and ML in Security in LinkedIn.
  - You can also send an e-mail to ksubbala@stevens.edu or dsaha@albany.edu

AIMLSec-SIG Monthly Virtual Seminar Series



Virtual Seminar Series

- ***Federated Learning in Unreliable and Resource-Constrained Cellular Wireless Networks***– Prof. Ekram Hossain, University of Manitoba, Canada at 11AM EDT.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Secure Code Execution on Untrusted Remote Devices*** – Prof. Gene Tsudik, UCI, USA. April28, 2021 at 1PM EDT.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording (Password: deMMW*E2)]
- ***Adversarial Machine Learning for Wireless Security in 5G and Beyond*** – Dr. Yalin Sagduyu, Intelligent Automation, Inc. (IAI), USA. March 26, 2021 at 10AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording (Password: +b^HF3CA)]
- ***A Quick Look at New Risks Facing Wireless Systems*** – Prof. Wade Trappe, Rutgers University, USA. February 25, 2021 at 10AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording (Password: %DJ3BF4^)]
- ***AI and Machine Leaning in Spectrum Sharing Security*** – Prof. Rose Qingyang Hu, Utah State University, USA. January 29, 2021 at 10AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording (Password: #+v4rh9V)]
- ***Deep Convolutional Neural Networks for Device Identification*** – Prof. Kaushik Chowdhury, Northeastern University, USA. December 16, 2020 at 9AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Physical Layer Security in Wireless Networks*** – Prof. Vincent Poor, Princeton University. November 17, 2020 at 9AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording (Password: %#=&2uej)]

Other Activities of AIMLSec-IG

- AIMLSec-IG will offer a tutorial in IEEE GLOBECOM 2021:
    - Deep Learning in Wireless Security and Privacy for Next-Generation Communication Systems -- K.P. Subbalskhmi, Yalin Sagduyu and Dola Saha
- AIMLSec-IG chair is an AE for IEEE Transactions on AI
- Group members regularly publish in IEEE Transactions on Cognitive Communications and Networks (TCCN)
- Group members have served as AE for IEEE TCCN