IEEE ComSoc
IEEE Communications Society

Technical Committee on Cognitive Networks (TCCN)

SIG in AI and Machine Learning in Security

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

Vice Chair:
Prof. Dola Saha,
University at Albany, SUNY
dsaha@albany.edu
https://www.albany.edu/faculty/dsaha/

Introduction to the AIMLSec-IG

- Currently about 450 members in LinkedIn
- To join AIMLSec-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

Virtual Seminar Series

- Started virtual seminars when traveling was restricted due to COVID
- Inaugural Speaker: Prof. Vincent Poor (Nov, 2020)

- ***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)]

Virtual Seminar Series - 2021

- ***Open Set Wireless Transmitter Authorization: Deep Learning Approaches and Practical Considerations***– Prof. Danijela Cabric, University of California, Los Angeles, USA. November 19, 2021 at 11AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Brainstorming Generative Adversarial Networks (BGANs): Framework and Application to Wireless Networks***– Prof. Walid Saad, Virginia Polytechnic Institute and State University, USA. October 22, 2021 at 10AM EDT.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Federated Learning in Unreliable and Resource-Constrained Cellular Wireless Networks***– Prof. Ekram Hossain, University of Manitoba, Canada, May 26, 2021 at 11AM EDT.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Secure Code Execution on Untrusted Remote Devices*** – Prof. Gene Tsudik, UCI, USA. April 28, 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)]

Virtual Seminar Series - 2022

- ***Securing and Optimizing Wireless Systems with AI-Native & Data-Driven Wireless Signal Processing in the Physical Layer*** – Dr. Tim O'Shea, CTO and Co-Founder at DeepSig Inc and a Research Assistant Professor at Virginia Tech, USA. December 13, 2022 at 10AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Blockchain Technology and its applications to the Internet of Things*** – Prof. Bhaskar Krishnamachari, University of Southern California, USA. November 11, 2022 at 11AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***AI and Privacy in Collaborative Spectrum Sharing: Perspectives from the Spectrum Collaboration Challenge and Beyond*** – Prof. John M. Shea, University of Florida, USA. April 27, 2022 at 10AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***6G for Information Security and Information Security for 6G*** – Prof. Aylin Yener, The Ohio State University, USA. March 30, 2022 at 11AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]
- ***Machine Learning Classification of RF Signals over Congested and Contested Spectrum: Algorithms and Experimentation*** – Prof. Marwan Krunz, University of Arizona, USA. February 23, 2022 at 11AM ET.
  [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]

- Topic or Speaker Suggestions: Please email us (ksubbala@stevens.edu or dsaha@albany.edu).

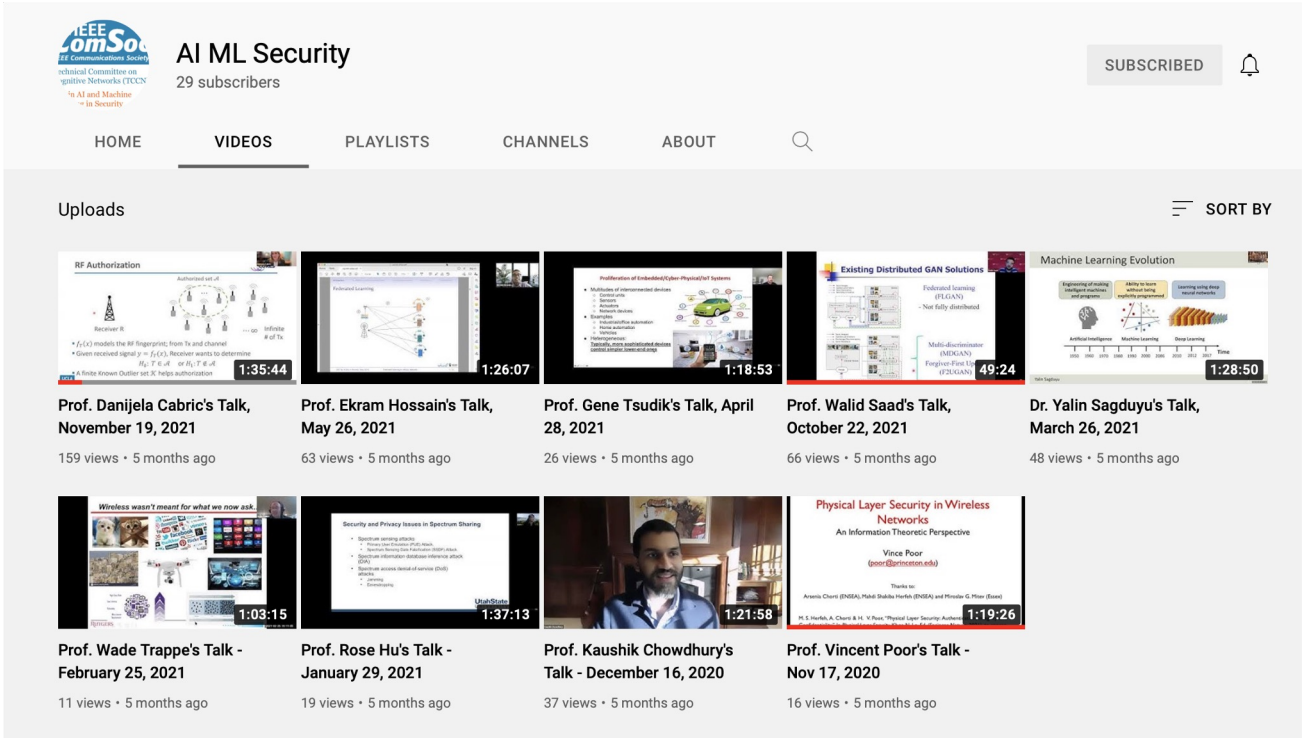
Virtual Seminar Series contd…

- ***5G and Future G Wireless Security*** – Dr. Arup Bhuyan, Idaho National Laboratory, USA**.** January 25, 2023 at 11AM ET. [Abstract and Author Bio] | [Registration] | [Slides] | [Recording]

- Topic or Speaker Suggestions: Please email us (ksubbala@stevens.edu or dsaha@albany.edu).
- We are putting together a team to lead other activities. If interested, get in touch with us.

YouTube Channel

- The YouTube Channel for the AIMLSec Webinar series is up and running.
- https://www.youtube.com/channel/UCsDvVnQCC5QclwpyL7J1FFA



Other Activities of AIMLSec-IG

- AIMLSec-IG Vice Chair is co-chairing Cognitive Radio and AI Enabled Networks Symposium at ICC 2024
- AIMLSec-IG chair is an AE for IEEE Transactions on AI
- AIMLSec-IG chair is an AE for IEEE Transactions on Neural Networks and Learning System (TNNLS)
- AIMLSec-IG chair is a Guest Editor in IEEE Transactions on AI on “Explainable and Interpretable AI”
- AIMLSec-IG vice-chair received Best Paper Award in DySPAN 2021
- Group members regularly publish in Cognitive Network Symposiums of both ICC and Globecom
- Group members regularly publish in IEEE Transactions on Cognitive Communications and Networks (TCCN)
- Group members have served as AE for IEEE TCCN