



Technical Committee on  
Cognitive Networks (TCCN)

SIG in AI and Machine  
Learning in Security

## Chair

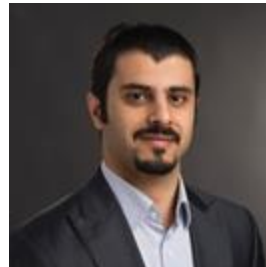


**Prof. K.P. (Suba) Subbalakshmi**  
Fellow National Academy of Inventors  
Stevens Institute of Technology,  
Jefferson Science Fellow  
Email: [ksubbala@stevens.edu](mailto:ksubbala@stevens.edu)  
Web: [www.kpsuba.com](http://www.kpsuba.com)

## Vice-Chairs



**Prof. Moinul Hossain**  
Assistant Professor  
George Mason University  
Email: [mhossa5@gmu.edu](mailto:mhossa5@gmu.edu)  
Web: [www.gmu.edu/profiles/mhossa5](http://www.gmu.edu/profiles/mhossa5)



**Prof. Hanif Rahbari**  
Associate Professor  
Rochester Institute of Technology  
Email: [hanif.rahbari@rit.edu](mailto:hanif.rahbari@rit.edu)  
Web: [www.rit.edu/wisplab/](http://www.rit.edu/wisplab/)



**Prof. Debashri Roy**  
Assistant Professor  
The University of Texas Arlington  
Email: [debashri.roy@uta.edu](mailto:debashri.roy@uta.edu)  
Web: [debashriroy.github.io/](http://debashriroy.github.io/)

# Introduction to the AIMLSec-IG

---

- We have a new website:  
<https://sites.google.com/view/ieee-comsoc-tccn-sig-aiml-sec>
- Currently about **551** members in LinkedIn
- To join AIMLSec-IG, use the LinkedIn group:
  - [http://www.linkedin.com/groups?home=&gid=5070076&trk=anet\\_ug\\_hm](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 email to us

# Hybrid Seminar

---

- A hybrid seminar was conducted jointly with Stevens Institute of Technology's 1st Symposium on Emerging Topics in Networks, Systems, and Cybersecurity
- ***Next-Generation AI for Next-Generation Wireless Networks***– Dr. Christo Kurumoottil Thomas, Virginia Tech, USA. August 13, 2024 at 11AM ET.

# 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 Learning 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.  
[\[Abstract and Author Bio\]](#) | [\[Registration\]](#) | [\[Slides\]](#) | [\[Recording\]](#)

# Virtual Seminar Series – 2023

---

- **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



# YouTube Channel

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

The screenshot shows the YouTube channel page for 'AI ML Security', which has 29 subscribers. The channel is subscribed to. The page displays a grid of video uploads, including:

- Prof. Danijela Cabric's Talk, November 19, 2021** (1:35:44)
- Prof. Ekram Hossain's Talk, May 26, 2021** (1:26:07)
- Prof. Gene Tsudik's Talk, April 28, 2021** (1:18:53)
- Prof. Walid Saad's Talk, October 22, 2021** (49:24)
- Dr. Yalin Sagduyu's Talk, March 26, 2021** (1:28:50)
- Prof. Wade Trappe's Talk - February 25, 2021** (1:03:15)
- Prof. Rose Hu's Talk - January 29, 2021** (1:37:13)
- Prof. Kaushik Chowdhury's Talk - December 16, 2020** (1:21:58)
- Prof. Vincent Poor's Talk - Nov 17, 2020** (1:19:26)



# Rising Star Symposium Series

---

- New initiative of the group.
- **Motivation**
  1. An opportunity for the community to hear from emerging scholars about the latest research and for the emerging scholars (senior PhD candidates and postdocs) to present their work to a border audience.
  1. The talks are intended to foster more mentorship, collaboration, and employment opportunities.
  1. The 45-minute talks are encouraged to be prepared in the form of “job talk” and interactively engage with the border audience.

# Rising Star Symposium Series

## (2023-2024)

---

1. ***Absolute Security in Terahertz Wireless Links*** - Dr. Chia-Yi Yeh, Massachusetts Institute of Technology (MIT) and Brown University, *Date: November 15, 2023.*
1. ***5G and 4G Coexistence Measurements Using Software-Defined Radio*** - Dr. Nadia Yoza Mitsuishi, National Institute of Standards and Technology, *Date: December 12, 2023.*
1. ***Machine Learning for Cyber Defense: From Network Security and Endpoint Security Perspectives*** - Mr. Mohammad Saidur Rahman, Rochester Institute of Technology, *Date: January 17, 2024.*
1. ***Toward In-Network ML on Programmable Network Devices*** - Mr. Changgang Zheng, University of Oxford, UK, *Date: February 13, 2024.*
1. ***The Road to Ultra-reliability in Future Mobile Networks*** - Dr. Andre Gomes, Commonwealth Cyber Initiative, USA, *Date: March 7, 2024.*
1. ***Deep Learning for Next-G Wireless Communications*** - Ms. Nasim Soltani, Northeastern University, USA, *Date: April 18, 2024.*
1. ***Next-Generation AI for Next-Generation Wireless Networks***- Dr. Christo Thomas, Virginia Tech, USA, *Date: August 13, 2024.*
1. ***GenAI-Based Chatbot for Early Dementia Intervention***- Dr. Junyuan Hong, UT Austin, USA, *Date: September 19, 2024.*
1. ***Towards Agent-based Autonomous Network Security***- Mr. Tao Li, NYU, USA, *Date: November 21, 2024.*

# Other Activities of AIMLSec-IG

---

- AIMLSec-IG Vice Chair, Prof. Saha, co-chaired Cognitive Radio and AI Enabled Networks Symposium at ICC 2024.
- AIMLSec-IG Vice Chairs, Prof. Hossain, Prof. Rahbari, Prof. Roy and Prof. Saha are TPC members for IEEE INFOCOM 2025. Prof. Rahbari was a **Distinguished** TPC member for IEEE INFOCOM 2024 too.
- AIMLSec-IG Chair, Prof. Suba, is an AE for IEEE Transactions on AI.
- AIMLSec-IG Chair, Prof. Suba, is an AE for IEEE Transactions on Neural Networks and Learning System (TNNLS).
- AIMLSec-IG Chair, Prof. Suba, is Lead Guest Editor for the Special Issue on “Explainable and Interpretable AI” in IEEE Transactions on AI.
- AIMLSec-IG Vice Chair, Prof. Roy, was a member of the organizing committee of MILCOM 2024, CCNC 2025, DySPAN 2024, and SMARTCOMP 2024.
- AIMLSec-IG Vice Chair, Prof. Saha is the workshop chair of DySPAN 2024.
- AIMLSec-IG Vice Chair, Prof. Saha is AE for IEEE Transactions on Cognitive Communications and Networking Journal.
- AIMLSec-IG Vice Chair, Prof. Saha is the editor for TCCN newsletter.
- AIMLSec-IG Vice Chair, Prof. Saha is the co-chair of N2Women organization.
- Group members regularly publish in Cognitive Network as well as Communication and Information System Security 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.

# Our Plan for 2025 and Beyond



**Absolute Security  
in High-Frequency Wireless Links**

Chia-Yi Yeh  
Postdoctoral Associate with MIT & Brown University  
2023.11.15  
TCO Security SIG's Monthly Virtual Doctoral Symposium Seminar Series



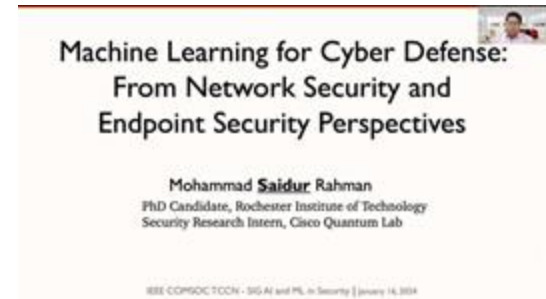
**5G and 4G Coexistence Measurement  
Using Software-Defined Radios**

Nadia Yoza-Mitsuishi, Yao Ma, Jason Coder

Shared Spectrum Metrology Group,  
Communications Technology Laboratory (CTL),  
National Institute of Standards and Technology (NIST)

IEEE ComSoc Technical Committee on Cognitive Networks  
Special Interest Group for AI and ML in Security  
December 12<sup>th</sup>, 2023

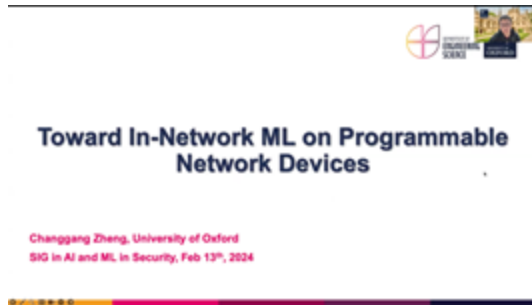
NIST National Institute of Standards and Technology U.S. Department of Commerce  
CTL



**Machine Learning for Cyber Defense:  
From Network Security and  
Endpoint Security Perspectives**

Mohammad **Saidur** Rahman  
PhD Candidate, Rochester Institute of Technology  
Security Research Intern, Cisco Quantum Lab

IEEE COMSOC TCCN - SIG AI and ML in Security | January 14, 2024



**Toward In-Network ML on Programmable  
Network Devices**

Changgang Zheng, University of Oxford  
SIG in AI and ML in Security, Feb 13<sup>th</sup>, 2024

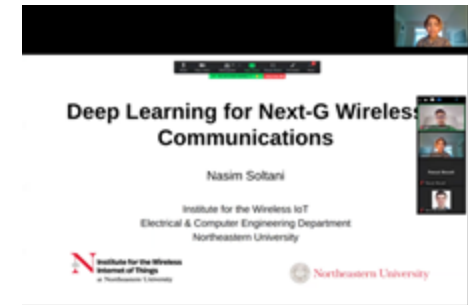


**The road to ultra-reliability in  
future mobile networks**

André Gomes, Ph.D.  
Postdoctoral Researcher  
Commonwealth Cyber Initiative @ Virginia Tech  
E. agomes@vt.edu | W. www.cwi.vt.edu

Acknowledgments:

VT VIRGINIA TECH  
NSF Award #2038866  
Special AI Community Collaborative, Networks and Security



**Deep Learning for Next-G Wireless  
Communications**

Nasim Soltani

Institute for the Wireless IoT  
Electrical & Computer Engineering Department  
Northeastern University

Institute for the Wireless Internet of Things at Northeastern University  
Northeastern University

Continue our effort to foster a seamless transition for young learners into the professional realm within our SIG interest area.

**Rising Star Suggestions: Please email us**