
# *Transforming the Resilience of Critical Infrastructure Systems and Communities*

***Resilience Week Objective:*** A Symposium dedicated to advancing the interdisciplinary dialog on policy and technologies that accelerate critical infrastructure and community resilience to unexpected and malicious threats.

## Session 04: *Wireless Security including 5G and Beyond*

### Session Chair


- Chair – Arupjyoti (Arup) Bhuyan, Idaho National Laboratory, arupjyoti.bhuyan@inl.gov
- Co-chair – Gurdip Singh, Syracuse University, gsingh06@syr.edu


### Authors' Schedule:

- Paper submission deadline: **July 1, 2019**
- Notification of acceptance: **September 9, 2019**

### Paper Submission:

- Full papers: must be submitted electronically through the electronic submission system.
- Written following IEEE format and limited to seven double column pages in a font no smaller than 10 points. Note that an extra page fee of $100 for each page (up to three additional pages) will apply to any camera-ready version exceeding the page limit.
- Work in progress and industry practice: written following IEEE format and limited to four double column pages, in a font no smaller than 10 points. Work-in-progress papers describe research that has not yet produced the results required for a full paper, but that due to its novelty and potential impact deserves to be shared with the community at an early stage.
- Accepted papers and work-in-progress papers will be submitted to IEEE for publication in Xplore.

### Session Abstract:


The session focusses on secure wireless communication for critical infrastructure systems and communities. While 5G brings significant improvements to speed, latency, and capability for massive M2M (machine to machine) communication, it is also bringing new security and resiliency challenges. This session invites papers on the new security and resiliency issue with wireless communications including 5G and beyond, and how to address them.


### Topics includes:

Secure Wireless Systems: Current wireless vulnerabilities and how to address them, Secure IoT with 5G, Security, Privacy and trust in wireless communications, Secure Communications for IoT of cyber-physical systems (including but not limited to: power transmission and distribution, control systems, industrial IoT, 5G Cellular drones etc.), Secure Edge Computing in 5G.