IEEE pimrc

IEEE International Symposium on Personal, Indoor and Mobile Radio Communications

9-12 September 2018 – Bologna, Italy

IEEE

IEEE ComSoc
IEEE Communications Society

Call for Special Session Papers

PIMRC 2018 Special Session SS12: Cybersecurity on the Fly

Date: Monday, Tuesday or Wednesday, September 10-12 (depending on overall schedule).
Special Session Organiser: Francesco Verde, University Federico II, Naples, Italy

Motivation and Background

Emerging infrastructure-free wireless applications include mobile ad hoc networks employing unmanned aerial vehicles (UAVs), which are often referred to as drones. Typically, when one thinks of cybersecurity, one thinks of using protection measures to our desktop computers, such as installing antivirus programs and using passcodes and pin numbers. Just like computers, UAVs are not exempt from a cyber-attack, since they fly without any human pilot on board and, thus, their flights are controlled either remotely by an operator or by on-board computer systems autonomously. Moreover, when the line of sight between a UAV and its ground control station (GCS) is lost, communications between them can be carried out via satellite links without encryption functionalities in many cases. Both small and large UAVs might be used by malicious users (e.g., criminals, terrorists, and business spies) to commit crimes, jeopardize public safety, invade secret databases, and so on, thus imposing new challenges in public security. Despite the recent interest tackled by UAV-based military and civilian applications, there does not appear to be a deep examination of cybersecurity issues for UAVs and related countermeasures.

We invite authors to present original and unpublished articles reporting cutting-edge research achievements in securing UAV-based communications. Potential topics include but are not limited to:

- GPS spoofing
- GPS, control stream, and data jamming
- Eavesdropping drones
- Video feed interception
- Virus attack on GCS
- Attacks targeting control streams between UAV and GCS
- Wi-Fi attacks
- Video replay attacks confusing the remote operator
- Simulation tools, benchmarks, and testbeds regarding cybersecurity for UAVs

Submission Guidelines

Prospective authors are invited to submit technical papers of their previously unpublished work. Accepted special session papers will be part of the Conference Proceedings and will be uploaded to IEEE Xplore. Papers should be submitted via EDAS; the links are available at http://pimrc2018.ieee-pimrc.org under "Authors". Papers should follow the same Author guidelines of the general symposium, which are available at http://pimrc2018.ieee-pimrc.org/authors/submission-guidelines/.

Key Dates

Paper submission:	**May 18, 2018**
Acceptance notification:	**June 15, 2018**
Final paper due:	**June 29, 2018**

The special session will be composed of one invited paper by Prof. Trung Q. Duong, School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, UK, and four papers accepted from open call after a full peer review process.