INCS-CoE

International Cybersecurity Center of Excellence
https://incs-coe.org

Security Challenges for UAVs

16 July (Wed) 12:00-13:30 pm London / 7:00-8:30 am EDT / 8:00-9:30 pm JST
https://hal.zoom.us/j/7376032434?pwd=azlzMncyK0tDOGhlUVRTVWZ3Z2RQdz09&omn=99977436650

Darren Hurley Smith, University of Kent (UK)

Darren Hurley-Smith is a Senior Lecturer in Information Security with School of Computing, University of Kent. He received the B.Eng. (Hons) in Hardware and Software Engineering (2012), and a PhD. in Autonomous Systems Network Security (2015) from the University of Greenwich. Since then, he has worked in a variety of security-related domains, including anti-ransomware strategy, random number generation, and secure mobile ad hoc networking (MANET) protocols. Darren is particularly interested in the impact of engineering and implementation choices on the security of everyday systems – particularly cutting-edge drone networks and autonomous vehicles. He focuses on resilient communications, especially where the safety of bystanders and parallel systems is paramount. His current work includes the development of secure MANET protocols for communication redundancy in UAV and Vehicle-to-Infrastructure scenarios.

Secure, Redundant Communications for Cooperative UAVs in Urban Airspace

Unmanned Aerial Vehicles (UAVs) are emerging as powerful tools in the future of delivery, offering speed, flexibility, and reduced reliance on ground transportation. As recent Beyond Visual Line of Sight (BvLoS) trials show increasing safety and reliability, the idea of drone-based delivery—once experimental—is quickly becoming viable at scale. But as UAVs take on more delivery roles, particularly in fleet-based operations with multiple owners, the challenge shifts from hardware capabilities to coordination and communication.

5G networks are often proposed as the ideal infrastructure for real-time communication, navigation, and traffic management of UAVs. However, 5G coverage is not guaranteed everywhere and can be disrupted by natural disasters or human interference. In these cases, how can drones safely complete deliveries or return to base without centralized infrastructure?

This talk outlines the key safety and communication requirements for heterogeneous UAV delivery fleets operating without access to telecom networks. It explores how drones can use Mobile Ad Hoc Networks (MANETs) to communicate directly with one another and continue functioning in disconnected or degraded environments. Special attention will be given to the security challenges of these decentralized networks and to emerging solutions, including a new generation of trust-based routing protocols, that offer promising ways to build resilient and secure drone delivery systems.

Panayiotis Kolios, University of Cyprus (Cyprus)

Panayiotis Kolios received both his BEng and PhD degrees in Telecommunications Engineering from King's College London in 2008 and 2011, respectively. He is currently an Assistant Professor at the Department of Computer Science, University of Cyprus, and a faculty member of the KIOS Center of Excellence. His research interests include both theory and application of networked intelligent systems. Particular emphasis is given to developing systems that deal with emergency management in which natural disasters, technological faults and man-made attacks could cause disruptions that need to be effectively handled. Tools used include primarily mathematical programming and machine learning in the context of multi-agent systems. Over the last several years Prof. Kolios managed to attract significant funding on the use of autonomous systems for disaster management (projects DG ECHO PREDICATE, SWIFTERS, LEAPFROG, AIDERS and ARTION), for border management (projects DG HOME CERETAB and REACTION), for intercepting rogue drones (projects H2020 CARAMEL and DG HOME PROTECTDOME) and for critical infrastructure inspection (KIOS Innovation Hub project in collaboration with the Electricity Authority of Cyprus). He is leading a team of 4 postdocs and 3 PhD researchers, as well as 7 researchers/software developers in addressing fundamental as well as practical challenges in the use of autonomous systems in the aforementioned application areas.

Measures/ counter-measures on the use of drones in security and public safety applications

Over the recent years, there have been tremendous advances in the development of drones / remotely piloted aircraft (RPAS) / unmanned aerial vehicles (UAVs). These vehicles have become extremely appealing, with a multitude of dual use applications. However, they can also potentially present major threats for security and public safety, especially when they fly across sensitive areas such as critical infrastructures and public spaces where a large number of people congregate.

This talk will review measure/counter-measure technologies used by pursuer/evader systems in the use of drones in various security and public safety scenarios. In addition, open challenges will be discussed, and promising future research avenues will be presented.

Aanjhan Ranganathan, Northeastern University (US)

Aanjhan Ranganathan is a tenured Associate Professor in the Khoury College of Computer Sciences at Northeastern University, USA. His research focuses on the security and privacy of wireless networks, with a strong emphasis on autonomous cyber-physical systems and smart ecosystems. His work regularly appears in top-tier venues such as NDSS, IEEE S&P, USENIX Security, and ACM MobiCom. He is a recipient of multiple prestigious honors, including the NSF CAREER Award, the Outstanding Dissertation Award from ETH Zurich, the Cyber Award from Armasuisse (Switzerland's Department of Defense), and the regional prize in the European Space Agency's Satellite Navigation Competition. Aanjhan actively serves the research community through program committee roles at major security conferences including CCS, NDSS, USENIX Security, and IEEE S&P, and has chaired several workshops and conference tracks. His

research is supported by agencies such as the National Science Foundation (NSF), the Office of Naval Research, the Army Research Laboratory, and Armasuisse.

Spoof, Defend, Deploy: Securing Full-Stack UAV Swarms

As UAV systems evolve from isolated drones to intelligent swarms, their reliance on GNSS and wireless communication makes them increasingly vulnerable to sophisticated RF-based attacks. This talk traces the progression of these threats—starting with practical GPS spoofing attacks on individual UAVs using minimal attacker knowledge [Sathaye et al., USENIX '22], and escalating to coordinated, stealthy swarm spoofing that subtly disrupts collective positioning and behavior [SwarmION GNSS '23]. In response, we introduce SemperFi [NDSS '22], a plug-and-play GPS spoofing mitigation framework that operates at the receiver level without relying on prior location information or external infrastructure. Moving beyond isolated threat models and defenses, we present PRISM—a modular, containerized testbed designed to simulate and deploy full-stack swarm UAV missions. Unlike traditional robotics simulators, PRISM integrates not just flight and autonomy, but realistic communication stacks and adversarial RF environments, enabling end-to-end experimentation from spoofing to swarm coordination. We conclude with Dyna5G, a lightweight 5G slicing case study that highlights how programmable communication resilience can complement spatial trust in contested airspace.