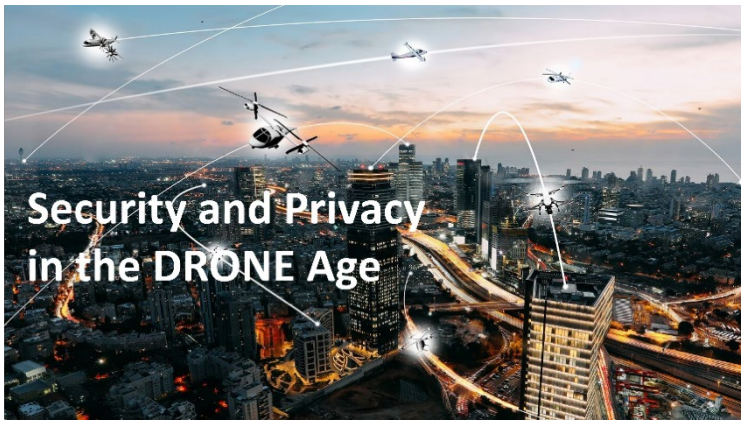
STAR Summer Camp: Security and Privacy in the Age of Drones

Professor: Dr. Cong Pu, *Computer Science*
Aims: Develop a lightweight authentication and key agreement protocol for drones.
Grade: 10-12 (Programming and Mathematics Knowledge)

Faculty Profile:
Dr. Cong Pu is leading the research project: "**Security and Privacy in the Age of Drones"**

Dr. Cong Pu is an Assistant Professor of Computer Science at Marshall University. His main research interest is wireless communication, IoT and cybersecurity. He is the recipient of the Helen DeVitt Jones Excellence in Graduate Teaching Award at Texas Tech University. He is a winner of 2017 Design for Delight (D4D) Innovation Challenge Competition as a faculty coach sponsored by Intuit Inc. He has been involved in numerous K-12 STEM initiatives including Open Education Resources Grant Award, and is currently a member of National Advisory Committee for the ETS Computer Science Praxis Exam. Please visit https://www.marshall.edu/cecs/profile/dr-cong-pu for more information.

Project Description:
Drones, or widely known as unmanned aerial vehicles (UAVs), have emerged as a key part of the fourth industrial revolution (often referred to as Industry 4.0), and provide an unprecedented opportunity to revolutionize mobility networks. Drones are no longer only limited to military applications, but they are also becoming progressively popular in various civilian application domains, such as disaster mitigation and relief, filmmaking and photography, delivery/fulfillment, agriculture/conservation, etc. For instance, during the Tokyo 2020 Olympics opening ceremony,



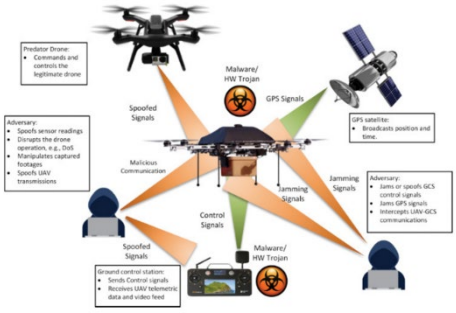
1,825 dazzling drones lighted up the sky and seamlessly became a revolving globe. In response to the COVID-19 pandemic, drones are well prepared to break out into a mass service and reduce direct person-to-person contact. In August 2021 the first COVID-19 vaccine drone delivery program in the United States was launched by North Carolina-based health system. The age of artificial intelligence, digital connectivity, automation and intelligent machines has arrived. Even though the ''Jetson lifestyle'' isn't upon us just yet, we envision that the advancements in drone technology will totally change the world as we know it in just a few short years.

Due to both financial and strategic information and value involved in aerial applications, the drone system is vulnerable to attacks that target either the cyber and/or physical elements, the interface

between them, the wireless link, or even a combination of multiple components. Since 2006, U.S. Customs and Border Protection has operated drones to patrol the U.S. borders with Mexico and Canada, watching for drug smugglers and unauthorized border crossers. However, it has been reported by the U.S. Department of Homeland Security and the U.S. Customs and Border Protection agency that drug traffickers have hacked their drones to cross the US-Mexican border illegally in January 2016. In addition, an adversary can send unauthorized commands to the drone to take its control from ground station, and then catch and withhold the drone. This is exactly how the ‘‘anti-drone-gun’’ operates, or hijacking the drone to have it go to an arbitrary waypoint. Therefore, investigating potential cyber threats against drones and designing the state-of-the-art security mechanisms are the top priority to ensure the cybersecurity of drone applications.

In this 4-week summer research camp, you will have an opportunity to understand the security and privacy issues of drones, learn various cryptographic techniques, and develop lightweight authentication and key agreement protocols for drones.

Weekly Activities Description:

Week 1: Security and Privacy Aspects in Drones
 Learning Objectives: You will learn - Drone System Architecture - Adversary Model - Security and Privacy Issues in Drones
Week 2: Cryptography
 Learning Objectives: You will learn - Cryptography Basic Principles - Cryptographic Data Integrity Algorithms - User Authentication
Week 3: Authentication and Key Agreement (AKA) Protocols

Learning Objectives: You will learn

- Overview of AKA Protocols

- Security Requirements and Constraints of AKA Protocols

- Design Lightweight AKA Protocols

Week 4: Experimental Study

Learning Objectives: You will learn

- AKA Protocol Implementation

- Simulation Environment and Testbed Setup

- Security and Performance Evaluation