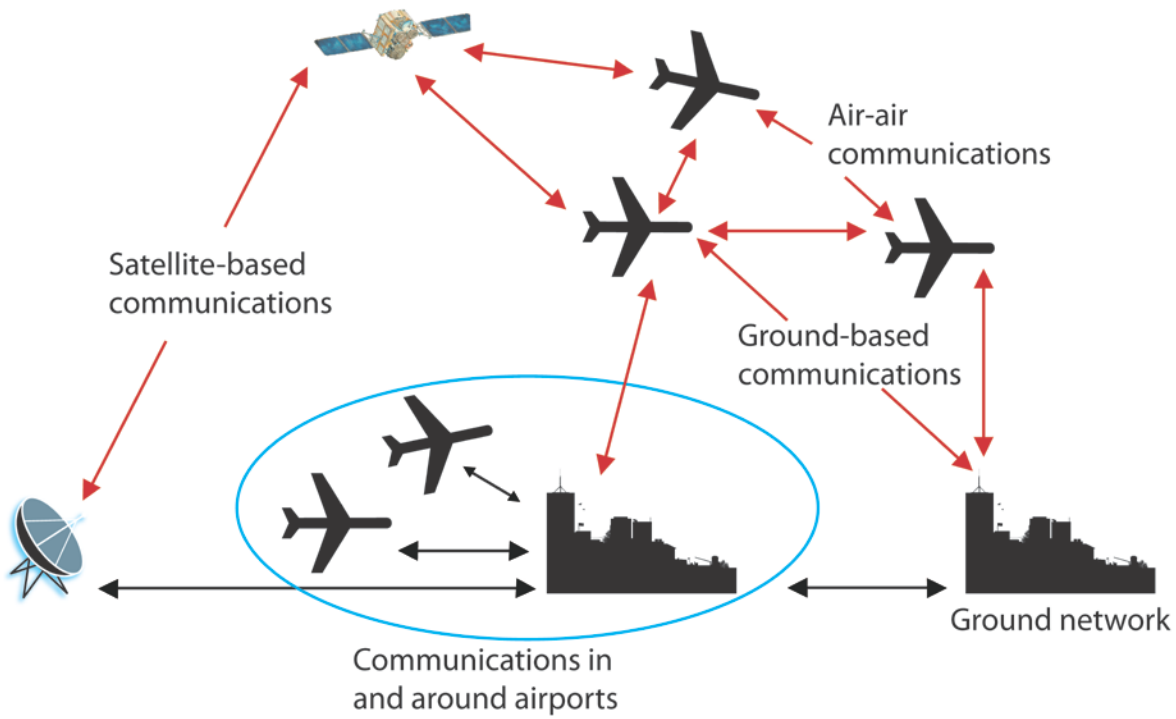
UAV Networks and Communications

KAMESH NAMUDURI IN COLLABORATION WITH

JEAN-MARC MOSCHETTA, SOFIE POLLIN, BERTOLD DEN BERGH, EVSEN YANMAZ, SAMIRA HAYAT, JAMES P. G, STERBENZ, NATASHA NEOGI, JAE H. KIM, ARUNABHA SEN, DAMIEN SAUVERON, SERGE CHAUMETTE, AND LEANNE HANSON

Outline of the Tutorial



- ✓ Introduction to UAV Networks
- ✓ Air to Ground Communications
- ✓ Air to Air Communications
- ✓ Aerial Networking
- ✓ Information Security
- ✓ Regulations
- ✓ Real World Applications

Introduction to UAV Networks

JEAN-MARC MOSCHETTA AND KAMESH NAMUDURI,

Introduction to UAVs and UAV Networks

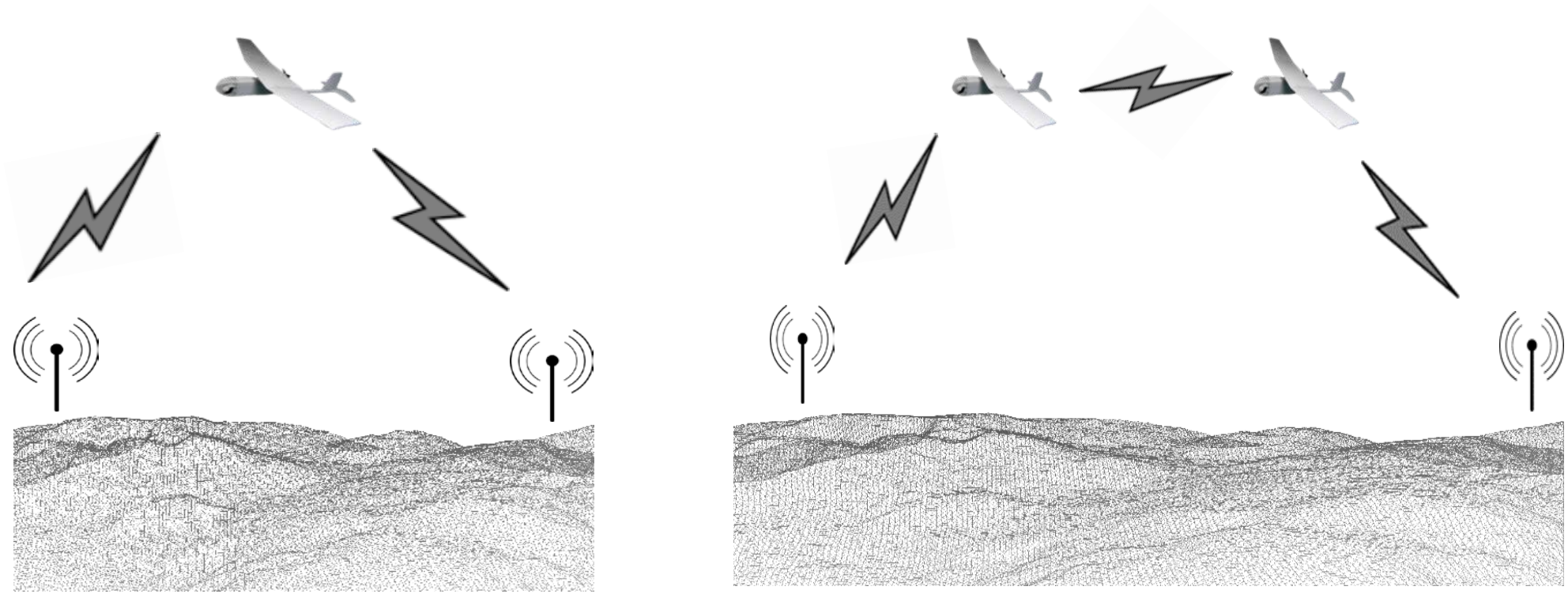
Terminology

- Remotely Piloted Aerial Systems
- Remotely Piloted Vehicles
- Unmanned Aircraft Systems

Classification

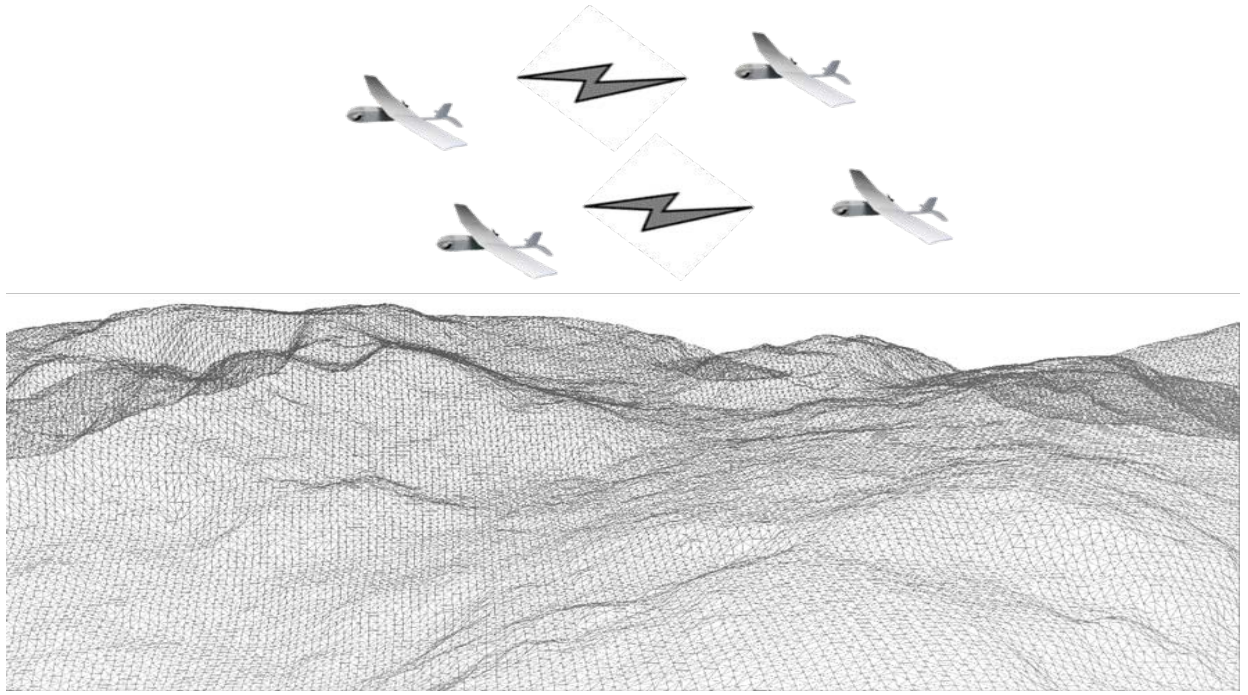
- Mission Capabilities (VTOL, Endurance, Indoor/Outdoor, Coverage, …)
- Size (Mini, Micro, etc)
- Altitude (High Altitude, Long Endurance or HALE)
- Functionality (Surveillance, Communications, ..)
- Wing-Type (Fixed, Flapping, Rotary, ..)

UAV Networks



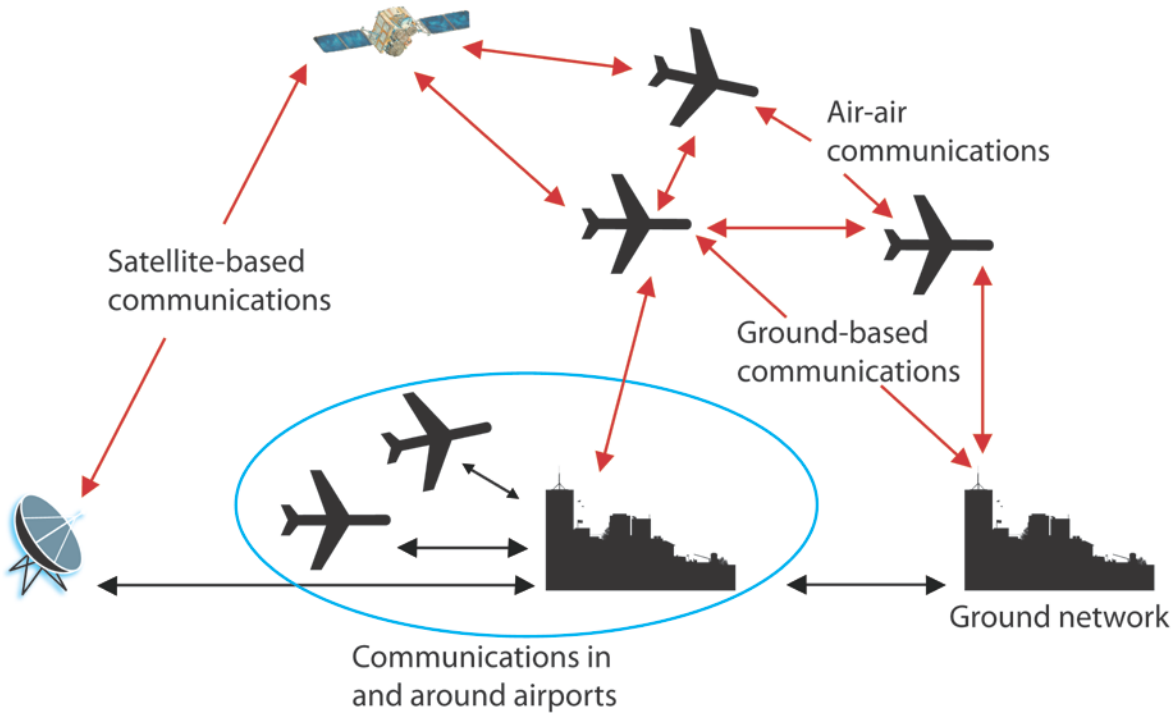
A UAV can serve as a relay node between a Transmitter -Receiver pair extending their communication range. The range can be further extended using multiple relays.

UAV Networks



Multiple UAVs forming an aerial mobile ad hoc network

UAV Networks



Airborne Network

UAV Networks

Mobility Models

- Random Direction
- Random WayPoint
- Gauss-Markov
- Smooth Turn

Existing Projects on UAV Networks

- Augnet (University of Colorado, Denver, 2004)
- UAVNet (University of Bern, 2012)

Air-to-Ground and Air-to-Air Communications

SOFIE POLLIN AND BERTOLD DEN BERGH

KU LEUVEN

Manned Aviation

- ✓ Primary Surveillance Radar
- ✓ Secondary Surveillance Radar
- ✓ Transponder
- ✓ Transponder Modes (A, C, and S)
- ✓ Cosec Squared Antenna Pattern
- ✓ Distance Measuring Equipment
- ✓ VHF Omnidirectional range
- ✓ Non-directional Beacon
- ✓ Instrument Landing System
- ✓ Voice Communication

Modernization

- ✓ Single European Sky ATM Research
- ✓ Next Generation National Airspace System

- ✓ Automatic Dependent Surveillance – Broadcast (ADS-B)
  - ✓ Situational Awareness
  - ✓ Improved Accuracy of Navigation
  - ✓ Identification
  - ✓ Improved Safety
  - ✓ Search and Rescue
  - ✓ Small Footprint
  - ✓ Cost

- ✓ Protocols for ADS-B Traffic
  - ✓ 1090 MHz Extended Squitter
  - ✓ Universal Access Transceiver

- ✓ VHF Data Link (VDL)
- ✓ L-band Digital Data Links
  - ✓ LDACS1
  - ✓ LDACS2

Exploring Multiple Antennas for UAV Communications

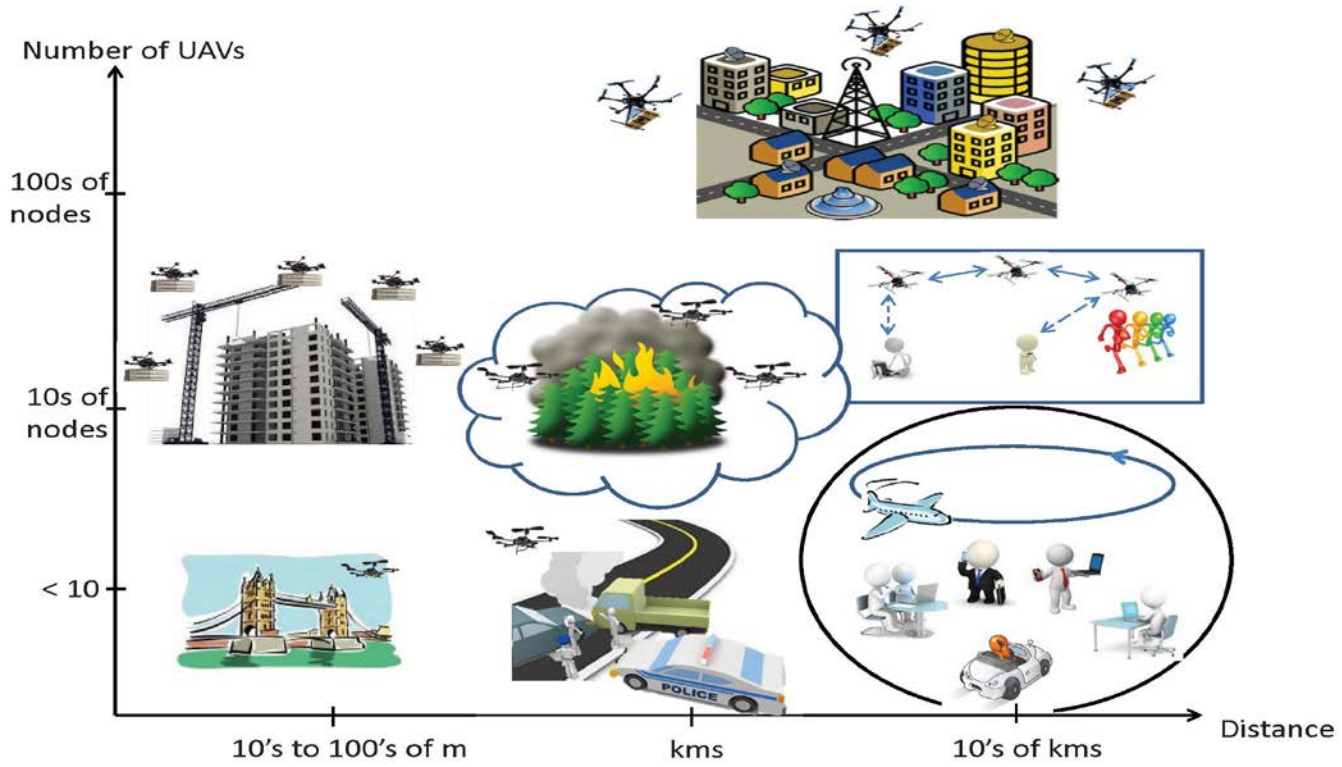
- ✓ Challenges
  - ✓ Small size of UAV frame
  - ✓ Lighter traffic from each UAV
  - ✓ Diversity of UAVs
  - ✓ Large number of simultaneous communication links
- ✓ Protocols
  - ✓ IEEE 802.11
  - ✓ GSM, GPRS, LTE
- ✓ Interference
  - ✓ From multiple terrestrial nodes
  - ✓ From other UAVs in the air

- ✓ Air-to-Air UAV Communications with Multiple Antennas
- ✓ Air-to-Ground UAV Communications with Multiple Antennas

Aerial WiFi Networks

EVSEN YANMAZ AND SAMIRA HAYAT

Applications of Aerial Networks



Application areas over a range of distances versus number of nodes

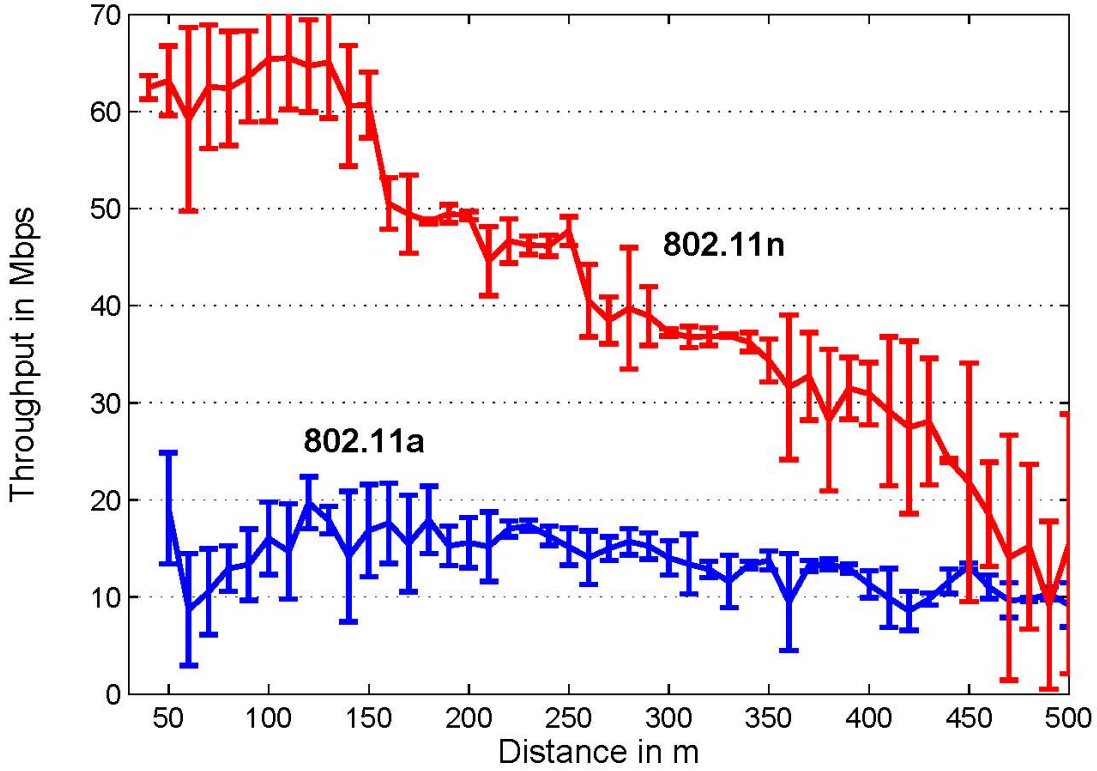
Aerial Networks

- ✓ Range of Applications
  - ✓ Public Safety
  - ✓ Network Provisioning for Emergency Situations
  - ✓ Mapping
  - ✓ Monitoring and Surveillance
- ✓ Options for Communication Links
  - ✓ WiFi (802.11x)
  - ✓ Zigbee (802.15)
  - ✓ 3G/LTE
  - ✓ Infrared
  - ✓ Optical
- ✓ Choice of Vehicles
  - ✓ Balloons (high endurance, limited altitude and range)
  - ✓ Fixed wing UAVs (larger area of coverage, longer flight times)
  - ✓ Rotary wing UAVs (hovering and maneuvering)
- ✓ Aerial Network Characteristics
  - ✓ 3D Nature
  - ✓ Mobility
  - ✓ Heterogeneous vehicles
  - ✓ Payload
  - ✓ Flight time

Communication Requirements of Aerial Networks

Application	Data Type	Frequency	Throughput	Traffic Type	Delay
Search and Rescue	Coordinated	> 1.7 Hz	4.8 Kb	Real time	50-100 ms
	Sensed	> 20 Hz	2 Mbs	Real time	50-100 ms
Monitoring & mapping	Coordinated	0.1 – 5 Hz	4.8 Kb	Periodic / DTN	
	Sensed	1 – 12 Hz	9.6 – 64 Kb	DTN	Can be offline
Visual tracking and surveillance	Coordinated	Similar to SAR	4.8 Kb	Real time	< 3 sec
	Sensed	> 10 Hz	1 Mbps	Real time	50-100 ms
Network provision	Coordination	Planned ahead	-	Periodic	-
	Sensed	30 – 50 Hz	12.2 - 384 Kbs	Real time	50-100 ms
Construction	Coordination	50 – 100 Hz	< 250 Kbs	Real time	-
Delivery of Goods	Coordination	20- 100 Hz	< 250 Kbs	Periodic	-

Real World Measurements



TCP Throughput over single hop links with infrastructure mode for P_tx = 12dBm

Regulations

NATASHS NEOGI AND ARUNABHA SEN

Model Aircraft Operations

- ✓ Fly below 400 feet and remain clear of surrounding obstacles
- ✓ Keep the aircraft within visual line of sight at all times
- ✓ Remain well clear of and do not interfere with manned aircraft operations
- ✓ Don't fly within 5 miles of an airport unless you contact the airport and control tower before flying
- ✓ Don't fly near people or stadiums
- ✓ Don't fly an aircraft that weighs more than 55 lbs
- ✓ Don't be careless or reckless with your unmanned aircraft – you could be fined for endangering people or other aircraft

Section 333 Exemption

"The Section 333 Exemption process provides operators who wish to pursue safe and legal entry into the NAS a competitive advantage in the UAS marketplace, thus discouraging illegal operations and improving safety. It is anticipated that this activity will result in significant economic benefits, and the FAA Administrator has identified this as a high priority project to address demand for civil operation of UAS for commercial purposes"

Air Space Over Private Property

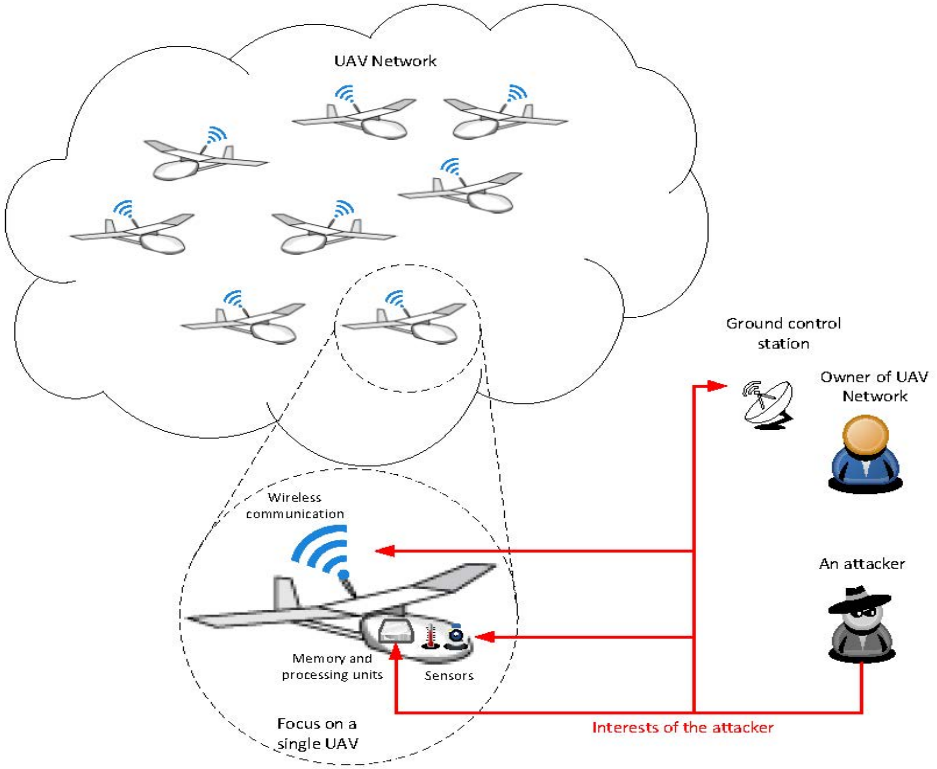
Which governs the airspace over my property – FAA regulations or local/state laws about unmanned aircraft systems (UAS)?

Under 49 United States Code 40103, the United States Government has exclusive sovereignty of airspace of the United States and the FAA has the authority to prescribe air traffic regulations on the flight of aircraft, including UAS. Whether Federal law preempts state or local requirements for UAS depends on the precise nature of those requirements. The Department of Transportation evaluates these laws or requirements on a case-by-case basis to make sure they don't conflict with FAA's authority to provide safe and efficient use of U.S. airspace.

Information Security

DAMIEN SAUVERON AND KAMESH NAMUDURI

Information Security



Threat Model

- ✓ Adversary
  - ✓ Is capable of capturing a flying UAV in a functional state
  - ✓ Able to attack while UAV is in flight
  - ✓ May access and change information
  - ✓ Disassemble the UAV to access internal memory
  - ✓ Reverse engineer to access proprietary information
  - ✓ Access embedded software
  - ✓ Install malicious software

Security Requirements

- ✓ To guard confidentiality of information
  - ✓ (SR1) UAV should be equipped with self-destruction mechanisms
  - ✓ (SR2) Information should be stored encrypted

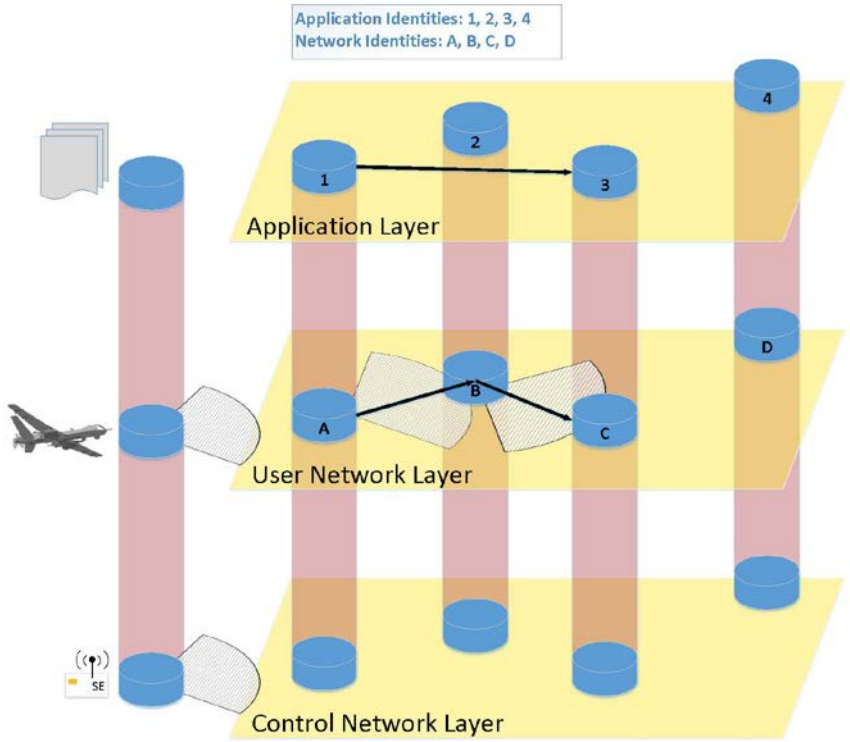
- ✓ To guard against side channel attacks, fault injection attacks, physical attacks and software attacks
  - ✓ (SR3) Processing unit should be tamper-resistant
  - ✓ (SR4) Secure key-management and cryptographic features should be used for information exchange
  - ✓ (SR5) Should provide remote authentication for software updates
  - ✓ (SR6) UAV must be subjected to evaluation and certification

Security Requirements

- ✓ To guard against spoofing and tampering with sensors such as GPS
  - ✓ (SR7) Use a secure positioning / location system
  - ✓ (SR8) Use redundant sensors that are tested before their use

- ✓ To guard against side network attacks
  - ✓ (SR9) All layers of the communication stack should include protection against DoS attacks
  - ✓ (SR10) Communication channels must include confidentiality and integrity strategies
  - ✓ (SR11) Communication channels should be opened only with authenticated entities
  - ✓ (SR12) If routing protocols are used, they must be secure

Security in UAV Swarms



UAV swarm using security elements, as proposed in (Akram et. al, 2014)

Security Requirements for UAV Swarms

- ✓ To guard against attacks on swarms
  - ✓ (SR13) Security of the entire swarm should be distributed on each UAV
  - ✓ (SR14) Each UAV should have a secure and unique ID
  - ✓ (SR15) Security of the swarm should rely on appropriate cryptographic functions
  - ✓ (SR16) Dynamic key sharing mechanisms should be employed

- ✓ To prevent loss of data in a swarm
  - ✓ (SR17) Redundancy mechanisms must be used

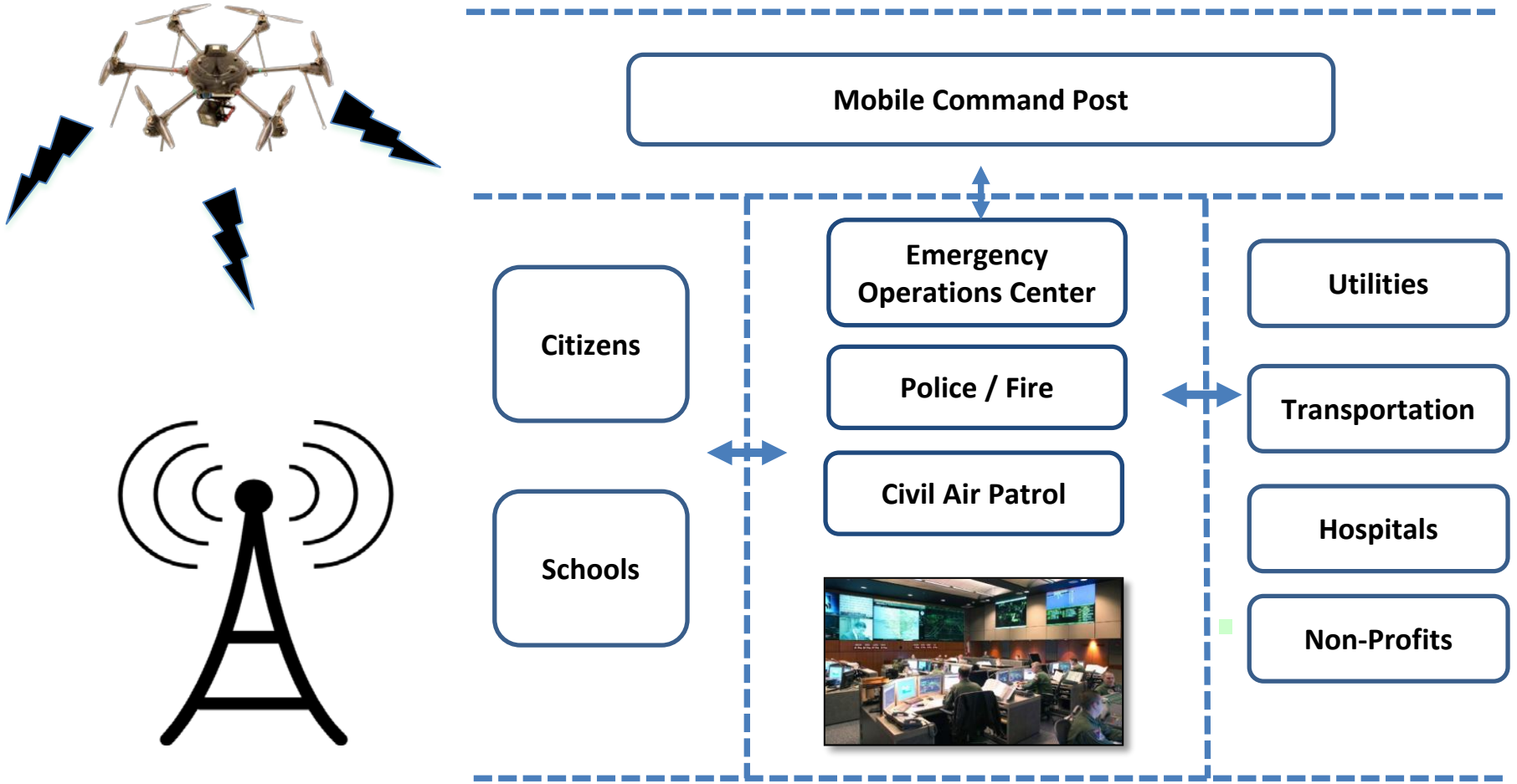
Security Requirements for RPS

- ✓ (SR 18) Ground-controller should be secure
- ✓ (SR 19) Command and Control links should be used to renew/refresh cryptographic keys from time to time
- ✓ (SR20) Communications links must be jam-resistant
- ✓ (SR21) Collected data should be sent to the ground station as soon as the link becomes available
- ✓ (SR22) Leaders should be redundant in multi-level fleets to avoid potential loss of collected data

Real World Applications

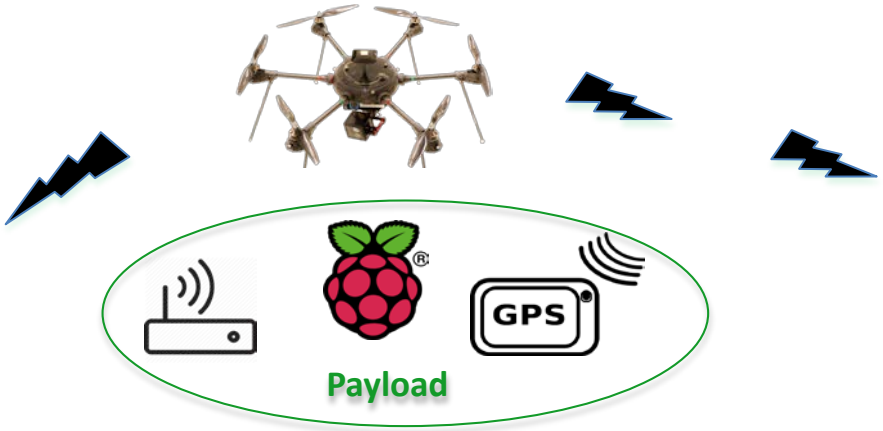
KAMESH NAMUDURI AND LEANNE HANSON

Integrating an Aerial Base Station with a City's Emergency Communication Grid



The Next-Generation Incident Command System (NICS)

GCTC Demonstration



Integration with Public Safety architectures

Voice Calls

Web-based situational awareness

GCTC Demonstration: Balloon-enabled Aerial Base Station

From Demonstration to Real World Applications
Requirements and Challenges

- **Deployment within the first 12-18 hours after a catastrophic event to temporarily restore critical communications, including broadband, for a period of 72-96 hours**
- **Mitigating interference with ongoing terrestrial communications**
- **Coordination with commercial operators to prevent harmful interference as commercial operations are restored**
- **Interoperability beyond communications for the primary Public Safety organizations of law enforcement, fire, and EMS. For example, over 50 agencies and organizations provided support for the May 2013 North Texas tornadoes**