Simulation and Modeling Concepts for Secure Airspace Operations

Dr. Banavar Sridhar
Universities Space Research Association (USRA)
@NASA Ames Research Center
Moffett Field, CA 94035

Mr. Kenneth Freeman
NASA Ames Research Center
Moffett Field, CA 94035

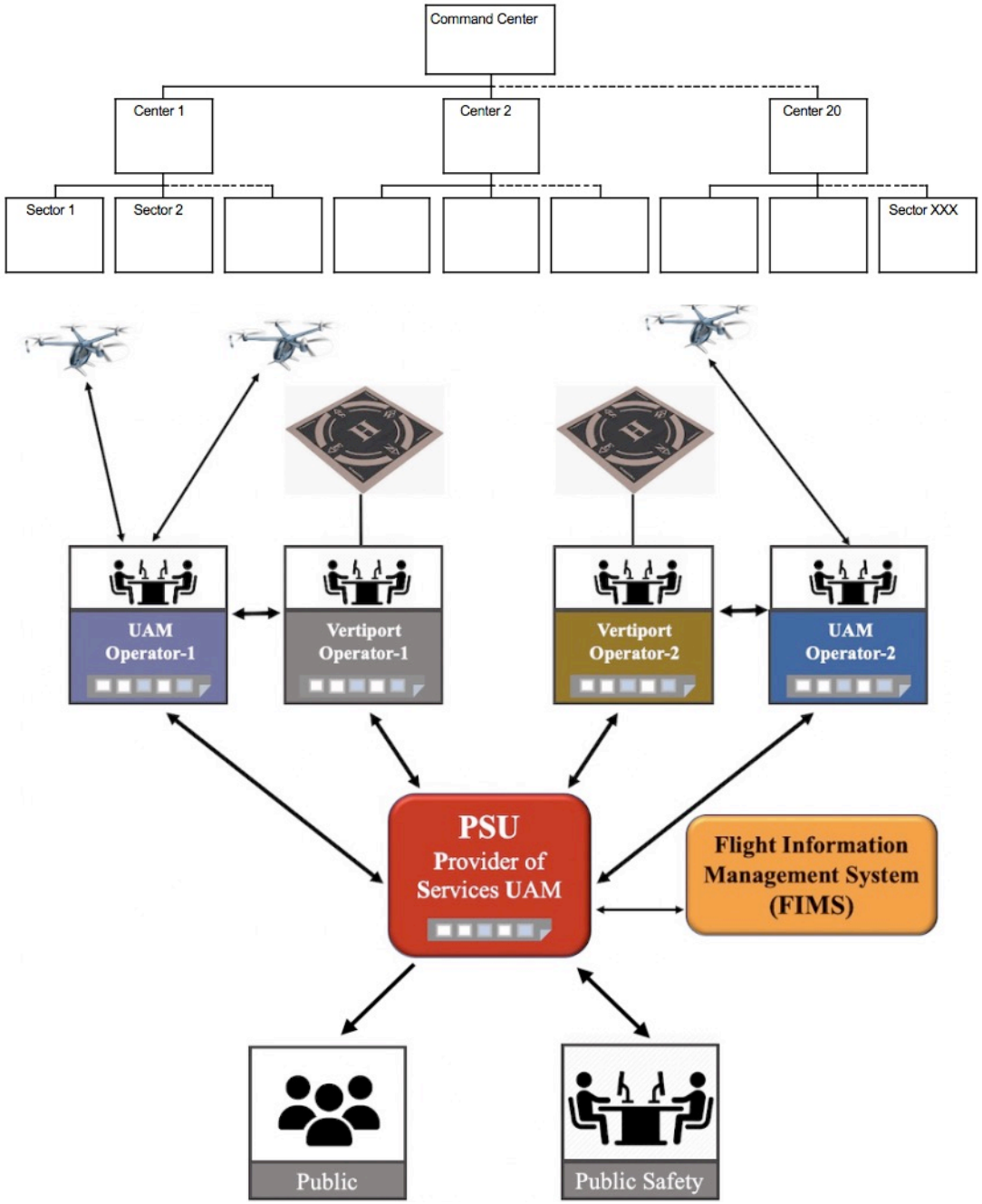
NSF-PIRE Workshop : US-Germany CPS Collaborations

Assured CPS Autonomy for 3d Urban Transportation:
Drones, Flying Cars and Beyond

June 9-10, 2021 | Virtual on Zoom

Urban Air Mobility (UAM)

Air Traffic Management (ATM) and UAM



- ATM is a hierarchical system with a centralized control and limited automation
- UAM is a distributed system, managed by multiple service providers, with evolving levels of automation with ATM functions provided as a service

What is this paper about?

- Data exchange is ubiquitous in UAM operations and conducted on public networks
- How to approach cybersecure UAM airspace operations?
- How to model the appropriate technology to understand trade-offs in cybersecure airspace operations as various services evolve with the maturity of UAM

Modeling Approach

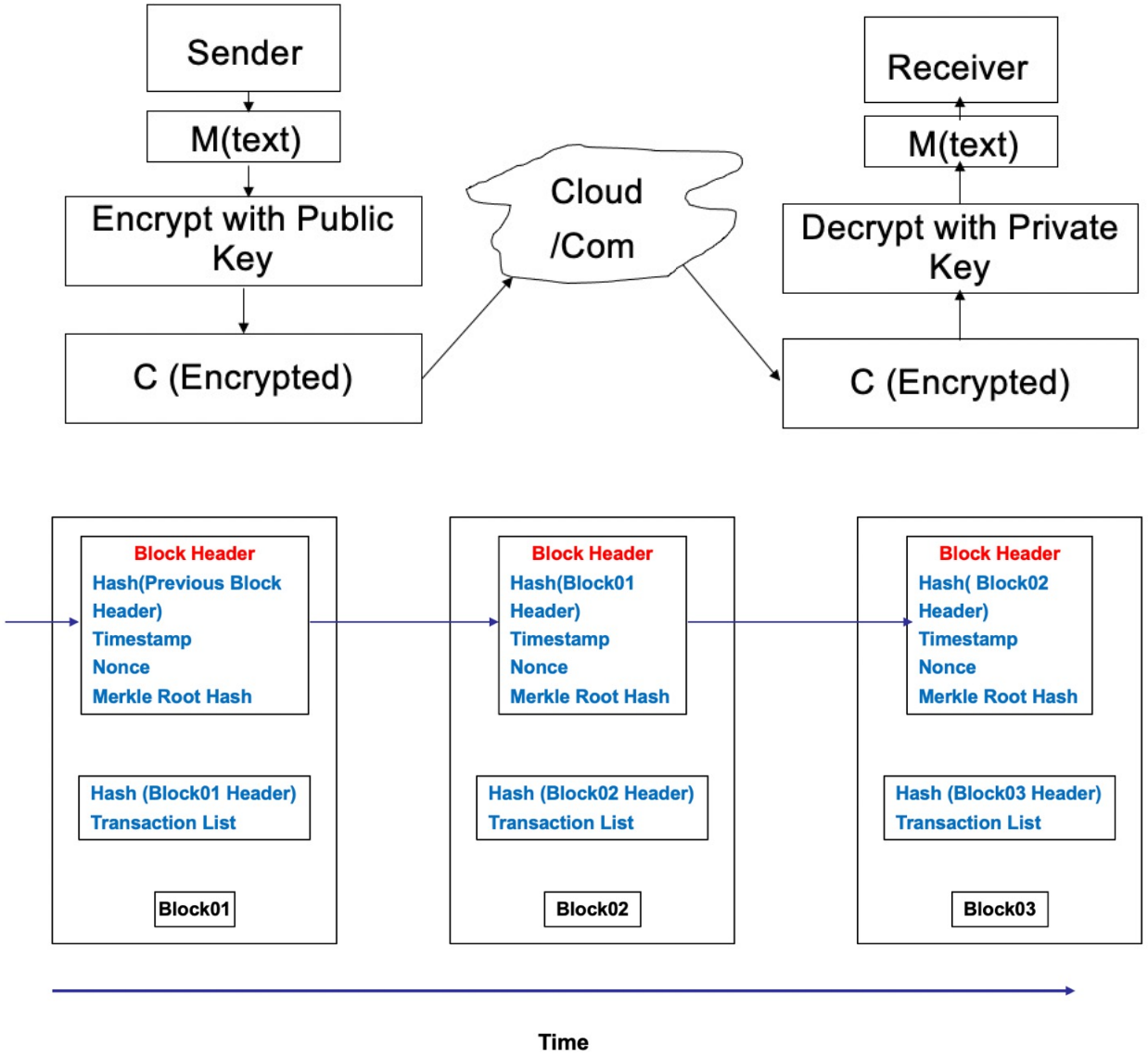
- Need for cybersecurity is present in all UAM operations
- Cybersecurity should be addressed at many different levels
  - Enterprise level, FAA, PSU, Vehicle, People
  - Level of security varies with the system risk associated with the function
- Review Advances in Hardware and Software Technologies affecting cybersecurity
- Build extensible modeling capability to make assessment of performance trade-offs in Secure Airspace Operations

Security Issues in Mobile Networks

- Current ATM: closed, regulated and operated by a single entity
- Wireless technology expected to be ubiquitous in UAM
  - ADS-B, GPS, 4G and 5G networks
  - 5G networks needed to support data exchange between vehicles
  - Some 5G technologies support mission critical activities with a latency of less than 5ms and 99.999% availability
- Data broadcast presents trade-offs between scale, latency and security in UAM applications
- Impact of security issues increase with higher levels of automation as the need for data exchange grows

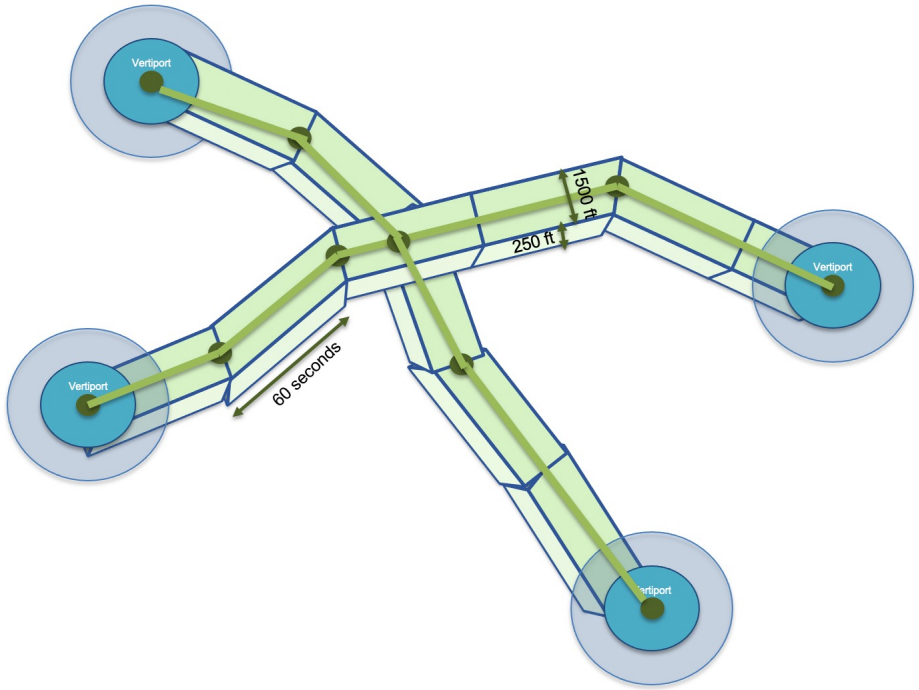
Cybersecurity Technologies

- Trusted Platform Module
- Encryption
- Blockchain Technology
- Virtual Information Fabric Infrastructure (VIFI)
- Machine Learning Techniques



Data exchange between PSUs

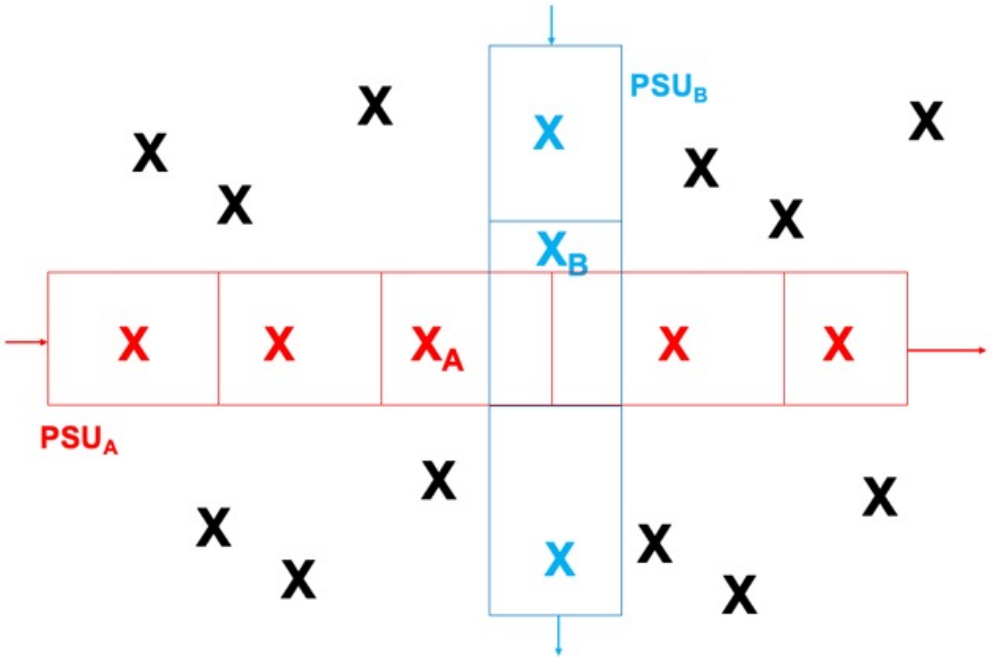
- Two PSUs: NASA-Uber Simulations*
  - Transit Based Operational Volume
  - 200 operations during a 40-minute interval
  - # of volumes/operation 30-70
  - # of position messages exchanged ~138,000
- Simulate immutable secure data exchange and storage using permissioned blockchain



*Lessons Learned: Using UTM Paradigm for Urban Air Mobility, Savita A. Verma, DASC 2020

Traffic levels and complexity

- Separation in a stream maintained by vehicles staying within their block
- If the blocks of aircraft in two different streams interact
  - X_A listens to verify all incoming messages, determine overlap, change its plan, generate and sign its broadcast
  - X_B reciprocates
- Amount of data transfer depends on the number of vertiports, traffic density and level of automation
- Creating scenarios to match maturity levels
  - 100 vehicles in level 4
  - 1000-10,000 and automation in levels 5-6



Concluding Remarks

- Cybersecurity is the responsibility of all organizations and individuals
  - should be addressed at each service level and during interaction between services
  - Enterprise level, FAA, PSU, Vehicle, People
  - Level of security varies with the system risk associated with the function
- Reviewed advances in Hardware and Software Technologies to support cybersecure operations
- Build extensible modeling capability to make assessment of performance trade-offs in Secure Airspace Operations
  - Authentication to anomaly detection