SESSION TS6 - 21 NOV 2019

DRONE SWARM NETWORKING

SESSION CHAIR: DAVID MUROTAKE
(HITACHI KOKUSAI ELECTRIC)

WInnComm 2019

Summit: 20-21 November 2019
Group Meetings: 18-19 November 2019
Atkinson Hall, UCSD, La Jolla, CA

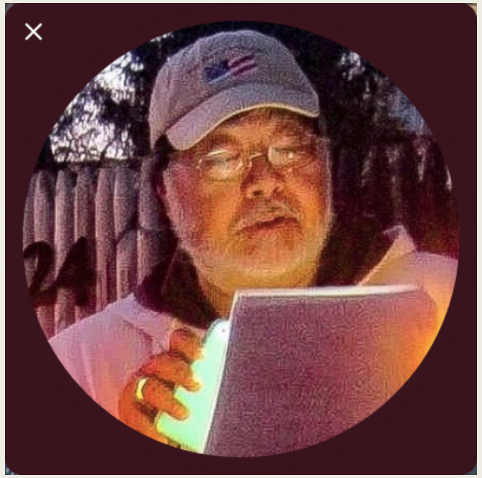
Plan of this Session

- 2:00 – 3:30 in Auditorium (followed by Break/Exhibits)
- Chair's Opening Remarks: Brief History. Business Case and Intellectual Property for Drone Swarms
- AS Testbed Architecture for 3D Mobility Research using Advanced Wireless Technology
  - *Vuk Marojevic (Mississippi State University, USA); Ismail Güvenç, Rudra Dutta and Mihail Sichitiu (North Carolina State University, USA); Jeffrey Reed (Virginia Tech, USA)*
- SwarmSense: Effective and Resilient Drone Swarm and Search for Disaster Response and Management Application
  - *Bo Ryu (EpiSys Science, USA); Cheolmin Jeon, Jeongsoo Ha, Hanbum Ko and Byeongman Lee (EpiSys Science, Korea)*

BRIEF HISTORY, BUSINESS CASE AND INTELLECTUAL PROPERTY FOR DRONE SWARM NETWORKING

David Murotake OCDS Ph.D.

Session Chair



- David K Murotake OCDS Ph.D.
- Adjunct Professor - Cybersecurity, University of St. Mary
- Phone Number: 603-321-6536
- Email: Murotake691@stmary.edu or david@murotake.com
- Education: *S.B./S.M. Electrical Engineering & Computer Science, MIT (1975/1977)*
  - *S.B. Humanities & Science (English Lit & Creative Writing), MIT (1977)*
  - *Ph.D., Management of Technological Innovation, MIT Sloan School (1990)*
- Founder, SCA Technica, Inc. and X4 Drone Lab, LLC

- Former NH State Representative and Nashua NH Board of Education
- Wireless Innovation Forum:
  - *Former Board of Directors, currently Software Defined Systems Steering Group*
  - *Past Vice-Chair, Technical Committee; Past Chair, Markets Committee*

2013: Paparazzi

Delft University

- Paparazzi drone swarm autopilot, originally developed and demonstrated by a Delft team to work for the Parrot AR Drone 2.0 with added GPS
- Remes, Hensen et al, “Paparazzi: how to make a swarm of Parrot AR Drones fly autonomously based on GPS”, International Micro Air Vehicle Conference and Flight Competition (IMAV2013), 17-20 September 2013, Toulouse, France

International Micro Air Vehicle Conference and Flight Competition (IMAV2013)
17-20 September 2013, Toulouse, France

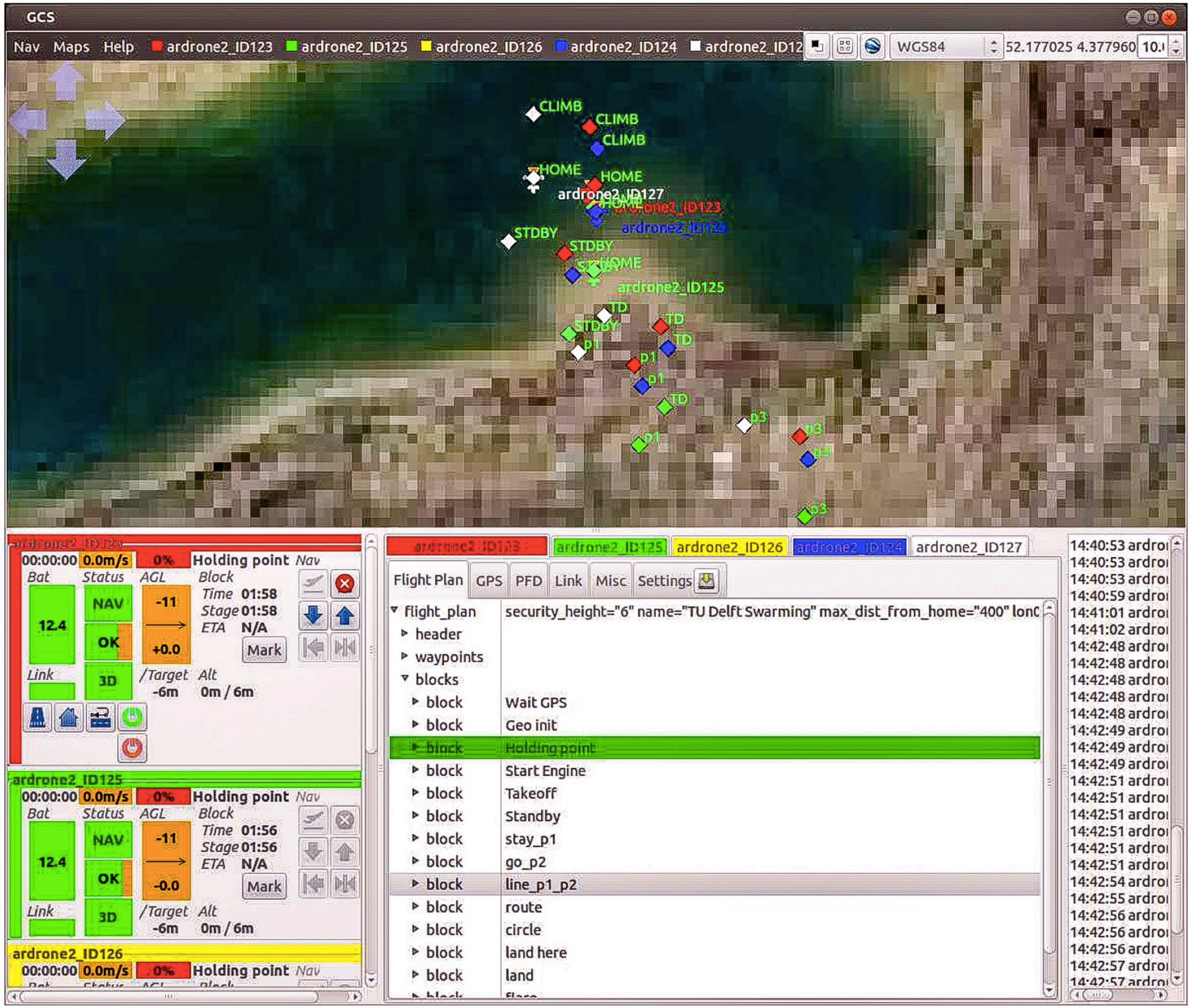
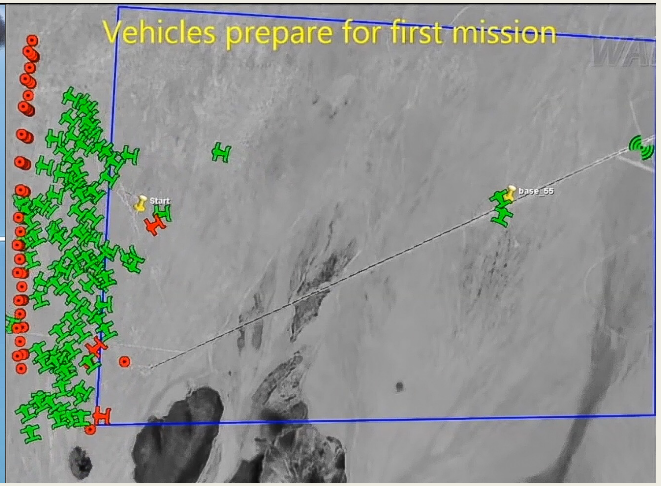


Figure 3: GCS with five AR drones.

2016: US DARPA SCO

100+ Perdix drones launched from F-16/F-18



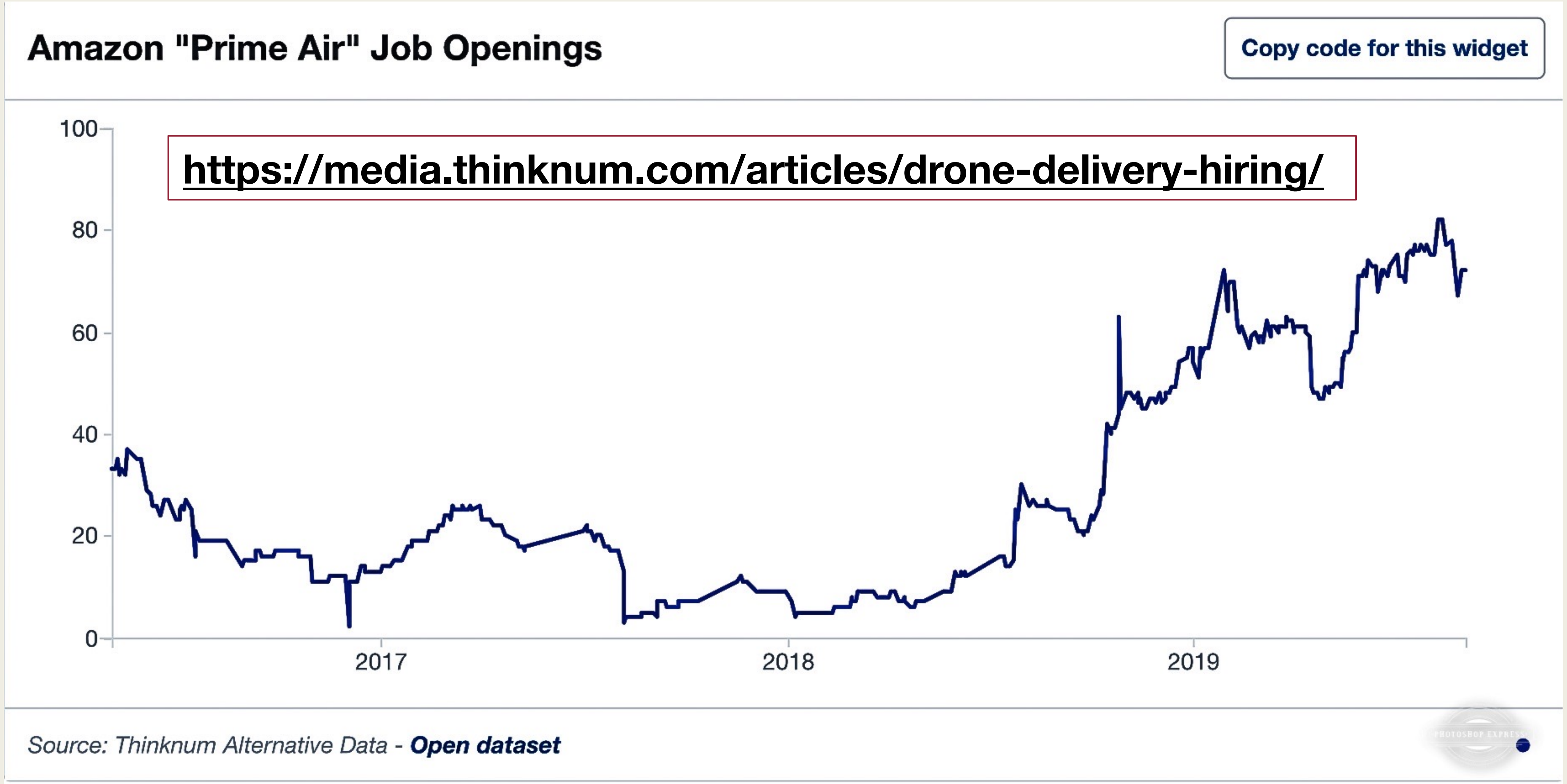
- **DARPA SCO** successfully launched a swarm of over 100 Perdix Drones from F-16, F-18 (October 2016)
- **Washington Post:** “Veil of secrecy lifted on Pentagon office planning ‘Avatar’ fighters and drone swarms” 8 March 2016
- https://www.washingtonpost.com/news/checkpoint/wp/2016/03/08/inside-the-secretive-pentagon-office-planning-skyborg-fighters-and-drone-swarms/

2018 Olympics: Intel

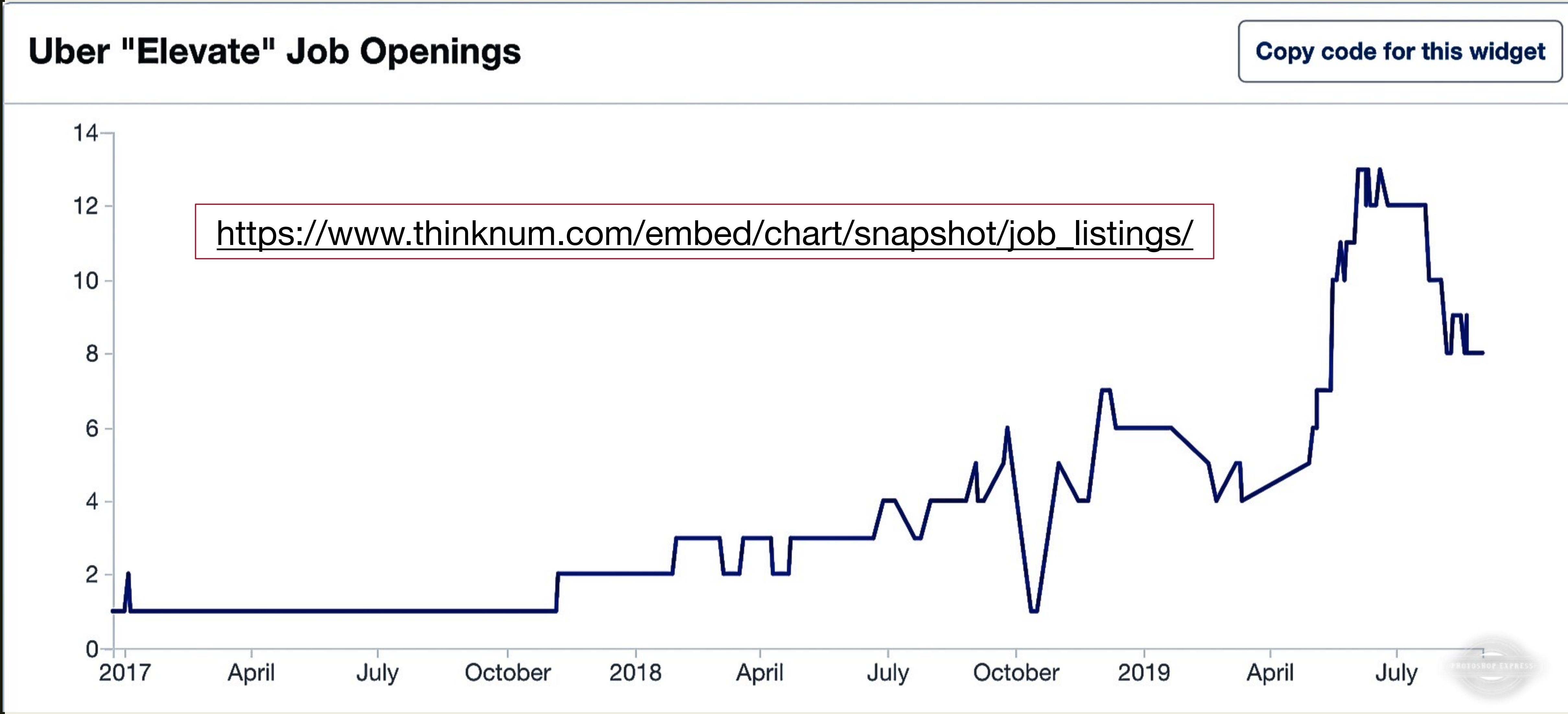
Flew over 1K drones in a drone swarm “dance”

- Intel successfully demonstrates drone swarms with over 1,000 drones in precision flight (2018 Olympics)
- By now drone swarms have replaced many fireworks displays around the world

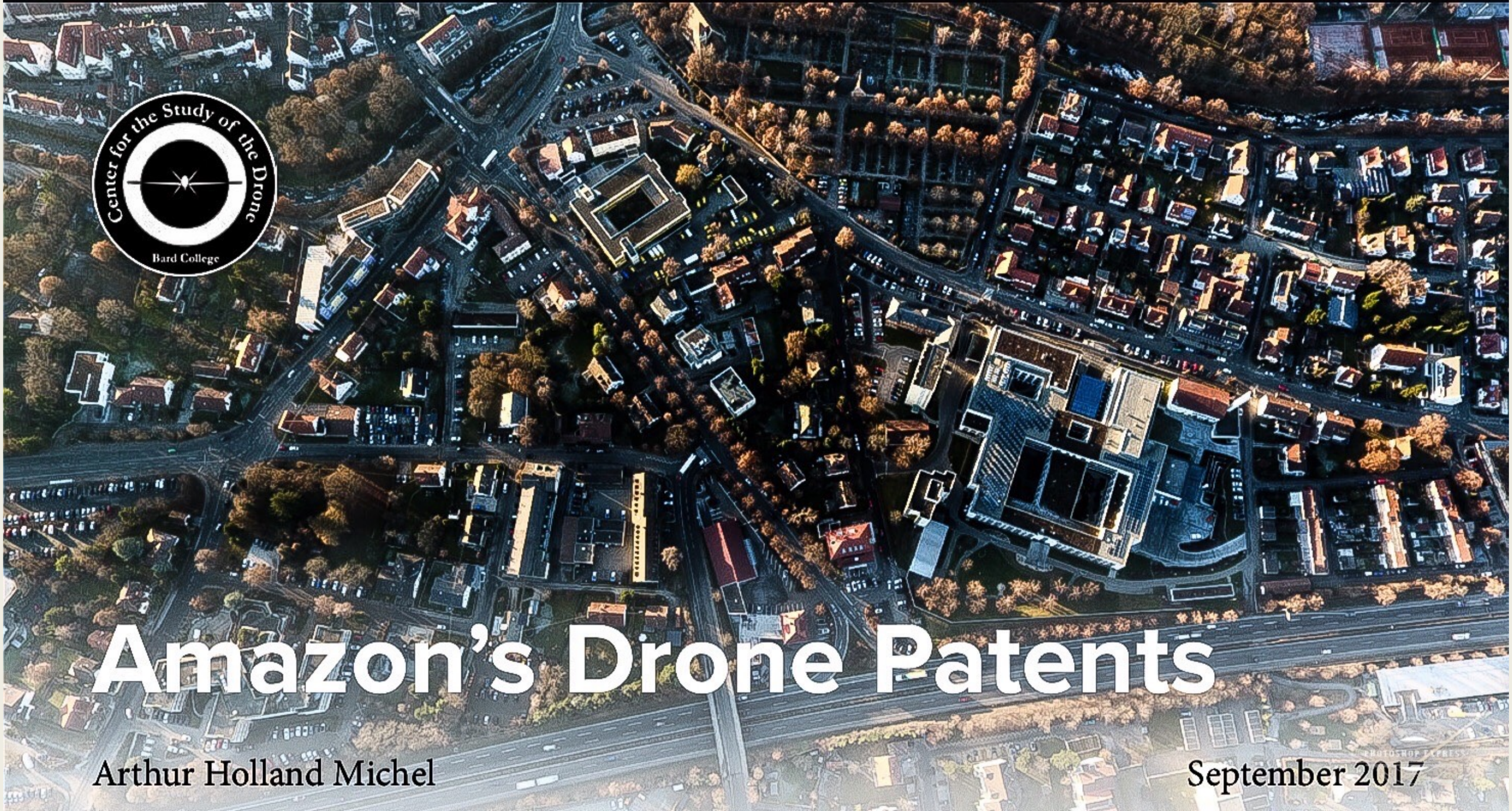
Amazon *Prime Air* Job Openings 2019



Uber *Elevate* Job Openings 2019



https://dronecenter.bard.edu/files/2017/09/CSD-Amazons-Drone-Patents-1.pdf



https://dronecenter.bard.edu/files/2017/09/CSD-Amazons-Drone-Patents-1.pdf

Table of Patents

Ref #	Patent #	Award Date	Patent Title	Abstract	Link
1	20150120094	4/30/2015	Unmanned Aerial Vehicle Delivery System	This disclosure describes an unmanned aerial vehicle ("UAV") configured to autonomously deliver items of inventory to various destinations. The UAV may receive inventory information and a destination location and autonomously retrieve the inventory from a location within a materials handling facility, compute a route from the materials handling facility to a destination and travel to the destination to deliver the inventory.	Source
2	US20150277440A1	10/1/2015	Sense and avoid for automated mobile vehicles	This disclosure describes an automated mobile vehicle that includes one or more distance determining elements configured to detect the presence of objects and to cause the automated mobile vehicle to alter its path to avoid the object. For example, a distance determining element may be incorporated into one or more of the motors of the automated mobile vehicle and configured to determine a distance to an object. Based on the determined distance, a path of the automated mobile vehicle may be altered.	Source
3	20150379876	12/31/2015	Object Avoidance for Automated Aerial Vehicles	This disclosure describes an automated aerial vehicle that includes one or more object detection elements configured to detect the presence of objects and an avoidance determining element configured to cause the automated aerial vehicle to automatically determine and execute an avoidance maneuver to avoid the objects. For example, an object may be detected and an avoidance maneuver determined based on a position of the object and an object vector representative of a direction and a magnitude of velocity of the object.	Source
4	9,305,280	5/5/2016	Airborne fulfillment center utilizing unmanned aerial vehicles for item delivery	Described is an airborne fulfillment center ("AFC") and the use of unmanned aerial vehicles ("UAV") to deliver items from the AFC to users. For example, the AFC may be an airship that remains at a high altitude (e.g., 45,000 feet) and UAVs with ordered items may be deployed from the AFC to deliver ordered items to user designated delivery locations. As the UAVs descend, they can navigate horizontally toward a user specified delivery location using little to no power, other than to stabilize the UAV and/or guide the direction of descent. Shuttles (smaller airships) may be used to replenish the AFC with inventory, UAVs, supplies, fuel, etc. Likewise, the shuttles may be utilized to transport workers to and from the AFC.	Source
5	2016077391	5/19/2016	Unmanned aerial vehicle configuration for extended flight	This disclosure describes a configuration of an unmanned aerial vehicle (UAV) that will facilitate extended flight duration. The UAV may have any number of lifting motors. For example, the UAV may include four lifting motors (also known as a quad-copter), eight lifting motors (octo-copter), etc. Likewise, to improve the efficiency of horizontal flight, the UAV also includes a pushing motor and propeller assembly that is oriented at approximately ninety degrees to one ormore of the lifting motors. When the UAV is moving horizontally, the pushing motor may be engaged and the pushing propeller will aid in the horizontal propulsion of the UAV.	Source
6	9,348,333	5/24/2016	Modular air delivery	Aspects of modular airborne delivery are described. When a shipping container is provided to an airborne carrier for delivery, the airborne carrier may assess weather across a route for airborne delivery of the shipping container, evaluate an approach to drop the shipping container at a delivery zone, and calculate a remaining amount of time until a target delivery time, for example. The airborne carrier may then select components to assemble a modular unmanned aerial vehicle (UAV) based on those or other factors, and assemble the UAV using the selected components. The modular UAV may then be directed to deliver the shipping container according to instructions from the airborne carrier. According to the concepts described herein, flexibility and other advantages may be achieved using modular UAVs for airborne delivery.	Source

Ref #	Patent #	Award Date	Patent Title	Abstract	Link
7	9,376,208	6/28/2016	On-board redundant power system for unmanned aerial vehicles	An unmanned aerial vehicle ("UAV") is configured with a redundant power generation system on-board the UAV. A redundant power system on-board the UAV can selectively utilize an auxiliary power source during operation and/or flight of the UAV. The power system on-board the UAV may include a battery and at least one auxiliary power source comprising a combustion engine. The combustion engine on-board the UAV may be selectively operated to charge the battery when a charge level of the battery is below a full charge level, and/or to power one or more propeller motors of the UAV.	Source
8	9,387,928	7/12/2016	Multi-use UAV docking station systems and methods	Systems and methods for providing a series of multiuse UAV docking stations are disclosed. The docking stations can be networked with a central control and a plurality of UAVs. The docking stations can include a number of services to facilitate both UAV guidance and maintenance and community acceptance and benefits. The docking stations can include package handling facilities and can act as a final destination or as a delivery hub. The docking stations can extend the range of UAVs by providing recharging/refueling stations for the UAVs. The docking stations can also include navigational aid to guide the UAVs to the docking stations and to provide routing information from the central control. The docking stations can be incorporated into existing structures such as cell towers, light and power poles, and buildings. The docking stations can also comprise standalone structures to provide additional services to underserved areas.	Source
9	20160229530	8/11/2016	Unmanned Aerial Vehicle Protective Frame Configuration	This disclosure describes a configuration of an unmanned aerial vehicle (UAV) that includes a frame that provides both structural support for the UAV and protection for foreign objects that may come into contact with the UAV. The UAV may have any number of lifting motors. For example, the UAV may include four lifting motors (also known as a quad-copter), eight lifting motors (octo-copter), etc. Likewise, to improve the efficiency of horizontal flight, the UAV may also include one or more pushing motor and propeller assemblies that are oriented at approximately ninety degrees to one or more of the lifting motors. When the UAV is moving horizontally, the pushing motor(s) may be engaged and the pushing propeller(s) will aid in the horizontal propulsion of the UAV.	Source
10	9,415,869	8/16/2016	Mobile Antenna Array	A plurality of UAVs may be operated in a fleet, each of the UAVs in the fleet being configured to work collectively to achieve one or more functions, such as to create a display or implement an antenna array. The fleet of UAVs may operate individually and/or may be coupled to one another to operate as a collective unit. In some embodiments, one or more UAVs in the fleet may operate individually, while two or more UAVs in the fleet may be connected to one another. In such embodiments, the individual UAVs and the connected UAVs may together comprise the fleet.	Source
11	9,422,055	8/23/2016	Unmanned aerial vehicle motor driving randomization for noise abatement	This disclosure is directed to varying a speed of one or more motors in an unmanned aerial vehicle (UAV) to reduce unwanted sound (i.e., noise) of the UAV. A UAV may include motors coupled with propellers to provide lift and propulsion to the UAV in various stages of flight, such as while ascending, descending, hovering, or transiting. The motors and propellers may generate noise, which may include a number of noise components such as tonal noise (e.g., a whining noise such as a whistle of a kettle at full boil) and broadband noise (e.g., a complex mixture of sounds of different frequencies, such as the sound of ocean surf). By varying the controls to the motors, such as by varying the speed or revolutions per minute (RPM) of a motor during operation by providing random or pseudo-random RPM variations, the UAV may generate a noise signature with reduced tonal noise.	Source

https://dronecenter.bard.edu/files/2017/09/CSD-Amazons-Drone-Patents-1.pdf

Amazon: Heavily Encrypted Mesh Networking

- Others have voiced concerns that Amazon's drones could be susceptible to hacking. In order to address these concerns, Amazon filed a patent (Ref. 18) for a system to protect its delivery drones from hacking and spoofing.
- According to the patent, which was awarded in 2016, the system would employ a **heavily encrypted mesh network** established among its drones that could evaluate whether any single drone within the network has been compromised.
- If the system detects that a drone has been hacked, it will direct the aircraft to land or hand control over to another airborne drone in the network.
- In another patent awarded in August 2017 (Ref. 61), the company proposes a technique for determining whether data received by a delivery drone can be trusted (if the drone determines that it cannot be trusted, it will ignore the data).

https://patents.google.com/patent/US9524648

Amazon Patent US9524648B1

Countermeasures for threats to an uncrewed autonomous vehicle

- **Abstract**
- Uncrewed autonomous vehicles ("UAVs") may navigate from one location to another location.
- Described herein are systems, devices, and methods providing countermeasures for threats that may compromise the UAVs.
- A plurality of UAVs may establish a mesh network to distribute information to one another.
- A first UAV may receive external data from a second UAV using the mesh network.
- The external data may be used to confirm or cross-check data such as location, heading, altitude, and so forth.
- Disagreement between data generated by the first UAV with external data from the second UAV may result in the determination that the first UAV is compromised.
- Remedial actions may be taken, such as the first UAV may be directed to a safe location to land or park, may receive commands from another UAV, and so forth.

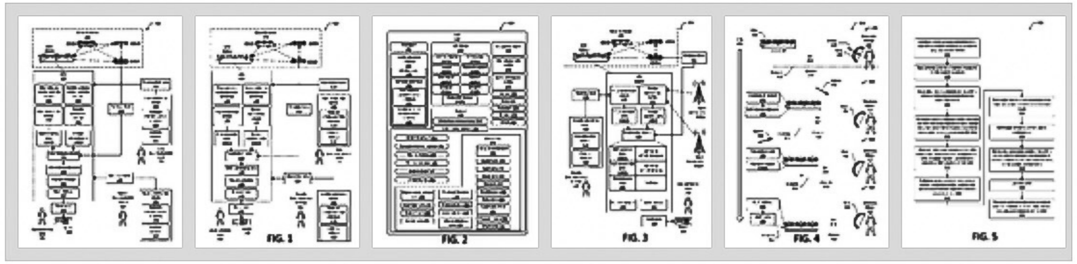
https://patents.google.com/patent/US9524648

Countermeasures for threats to an uncrewed autonomous vehicle

Abstract

Uncrewed autonomous vehicles ("UAVs") may navigate from one location to another location. Described herein are systems, devices, and methods providing countermeasures for threats that may compromise the UAVs. A plurality of UAVs may establish a mesh network to distribute information to one another. A first UAV may receive external data from a second UAV using the mesh network. The external data may be used to confirm or cross-check data such as location, heading, altitude, and so forth. Disagreement between data generated by the first UAV with external data from the second UAV may result in the determination that the first UAV is compromised. Remedial actions may be taken, such as the first UAV may be directed to a safe location to land or park, may receive commands from another UAV, and so forth.

Images (13)



Classifications

G08G5/0082 Surveillance aids for monitoring traffic from a ground station

View 8 more classifications

US9524648B1

United States

Download PDF | Find Prior Art | Similar

Inventor: Varadarajan Gopalakrishnan, Jesper Mikael Johansson, James Domit Mackraz, Jon Arron McClintock, Brandon William Porter, Andrew Jay Roths

Current Assignee : Amazon Technologies Inc

Worldwide applications

2014 • US

Application US14/543,198 events

- **2014-11-17** • Application filed by Amazon Technologies Inc
- **2014-11-17** • Priority to US14/543,198
- 2015-09-30 • Assigned to AMAZON TECHNOLOGIES, INC.
- **2016-12-20** • Application granted
- **2016-12-20** • Publication of US9524648B1
- **2019-11-20** • Application status is Active
- **2035-01-26** • Adjusted expiration

Info: Patent citations (11), Cited by (40), Legal events

IBM Patent US9651945B1

Dynamic management system, method, and recording medium for cognitive drone-swarms

A method, system, and recording medium including

- a mission receiving device configured to receive a mission for the drone-swarm based on a user input,
- a drone and pattern recruiting device configured to recruit a plurality of drones based on the mission,
- and a flocking goal device configured to arrange the plurality of drones in the **drone-swarm** in a pattern to satisfy the mission.

patents.google.com

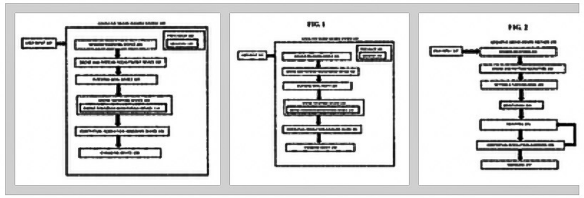
https://patentimages.storage.googleapis.com/a0/f2/4c/f086a9545cfc37/US9651945.pdf

Dynamic management system, method, and recording medium for cognitive drone-swarms

Abstract

A method, system, and recording medium including a mission receiving device configured to receive a mission for the drone-swarm based on a user input, a drone and pattern recruiting device configured to recruit a plurality of drones based on the mission, and a flocking goal device configured to arrange the plurality of drones in the drone-swarm in a pattern to satisfy the mission.

Images (6)



Classifications

G08G5/0039 Modification of a flight plan

View 13 more classifications

US9651945B1
United States

Download PDF
Find Prior Art
Similar

Inventor: Thomas David Erickson, Rogerio Schmidt Feris, Clifford A. Pickover

Current Assignee : International Business Machines Corp

Worldwide applications

2015 • US 2017 • US

Application US14/930,806 events

2015-11-03	Application filed by International Business Machines Corp
2015-11-03	Priority to US14/930,806
2015-11-03	Assigned to INTERNATIONAL BUSINESS MACHINES CORPORATION
2017-05-04	Publication of US20170123418A1
2017-05-16	Application granted
2017-05-16	Publication of US9651945B1
2019-11-20	Application status is Active
2035-11-03	Anticipated expiration

Info: Patent citations (3), Cited by (6), Legal events, Similar documents, Priority https://www.intel.com/content/www/us/en/drones/solutions/intel-insight-platform.html

Intel® Insight Platform

THE INTEL® INSIGHT PLATFORM

The Intel® Insight Platform helps you store, organize, process, and harness the growing amounts of visual data associated with large assets and sites spread around the world, in a collaborative environment designed to enable geographically dispersed teams in complex multi-party projects. With its open cloud infrastructure you can develop and deploy analytics and applications at scale with the help of Intel and other ecosystem players.

TRANSFORM YOUR DATA INTO ACTIONABLE INSIGHTS

Businesses that are managing high value assets, critical infrastructure, or large sites spread across geographies, are amassing large amounts of data from multiple sources. Unlock the power of your visual and geospatial data and use it to help inform critical business decisions.

https://www.intel.com/content/www/us/en/technology-innovation/aerial-technology-light-show.html

https://www.natlawreview.com/article/cybersecurity-considerations-drones

THE
NATIONAL LAW REVIEW
November 18, 2019

Cybersecurity Considerations for Drones

Thursday, November 7, 2019

The Federal Aviation Administration (FAA) estimates that by 2023 there will be more than 835,000 commercial drones in the United States. As the use of drones for many commercial purposes (such as aerial inspections, utility projects, monitoring real estate and construction activities) increases, more and more organizations will consider how to integrate these devices into existing networks and systems. However, these organizations must also consider how to limit the cybersecurity and privacy risks associated with the data collected by the drones.

Drones operate by using software or firmware. Drone operators use computers and mobile devices to run drone applications. Drones store data (on the drone itself in many cases) and often communicate via wireless connections to ground stations and operators below. What are the risks? Well, hackers are already exploiting drone software and firmware vulnerabilities to take over the drone and gain access to the connected system and network (and the data stored on the drone). Malware is often embedded in drone software and can compromise not only the date collected on the drone, but the systems that the drone, software or connected devices are linked to.

ARTICLE BY
Kathryn M. Rattigan
Robinson & Cole LLP
Data Privacy + Security Insider
Robinson+Cole

Utilities & Transport
Communications, Media & Internet
Consumer Protection
All Federal

PRINTER-FRIENDLY
EMAIL THIS ARTICLE
DOWNLOAD PDF
REPRINTS & PERMISSIONS

RELATED ARTICLES

Energy Sector's Reliance on IoT Increases Cyber Vulnerabilities

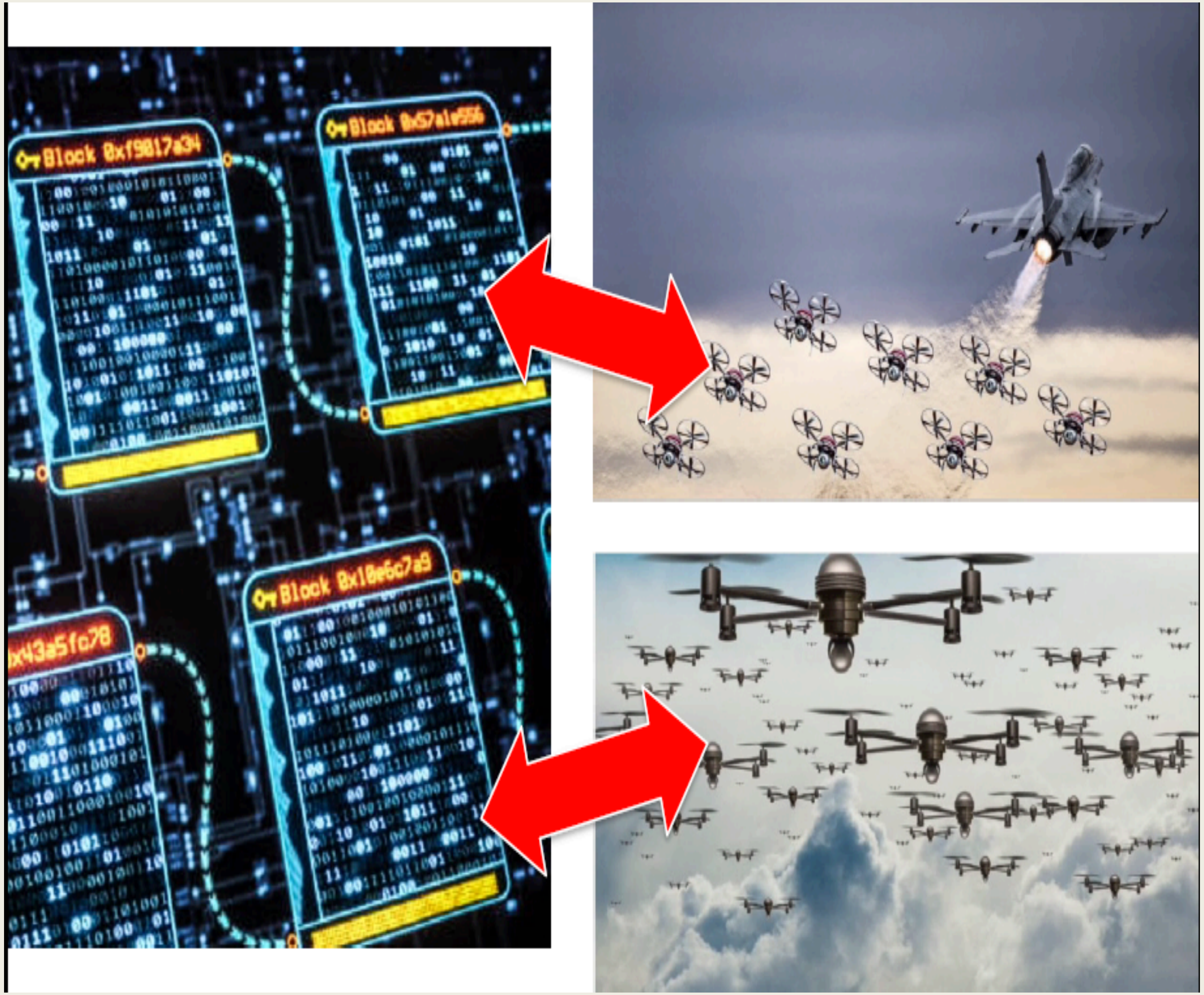
FBI Warns of E-Skimming Threats

Telecom Alert — DC Circuit Net Neutrality Ruling; CA 911 Outage Reporting; CAF Requirements, VoIP, and 800 MHz Re-Banding to be Considered at October Open Meeting; NHTSA Awards $1.7 Million in 911 Grants — Vol. XVI, Issue 40

Cybersecurity and the Electric Grid – New GAO Report Identifies Actions Needed to Address Cybersecurity Risks

Where are we headed tomorrow?

- Heavily encrypted mesh networks (commercial)
- LPI/LPD “Stealthy” Airborne Networks (military)
- Propagation models
- Blockchains
- Cybersecurity



THANK YOU!

AS TESTBED ARCHITECTURE FOR 3D MOBILITY RESEARCH USING ADVANCED WIRELESS TECHNOLOGY

Vuk Marojevic (Mississippi State University, USA); Ismail Güvenç,
Rudra Dutta and Mihail Sichitiu (North Carolina State University, USA);
Jeffrey Reed (Virginia Tech, USA)

Speaker Biography
PROF Jeff Reed, Virginia Tech

Dr. Jeffrey H. Reed is the founder of *Wireless @ Virginia Tech,* and served as its Director until 2014. He is the Founding Faculty member of the Ted and Karyn Hume Center for National Security and Technology and served as its interim Director when founded in 2010. Currently he is the Interim Director of the Commonwealth Cyber Initiative (CCI). He is the author of five books on radio design and wireless communications. He is co-founder of Cognitive Radio Technologies, a company commercializing of the cognitive radio technologies; Federated Wireless, a company developing spectrum sharing technologies; and PFP Cybersecurity, a company specializing in security for embedded systems. In 2005, Dr. Reed became Fellow to the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education. In 2013 he was awarded the International Achievement Award by the Wireless Innovations Forum. In 2012 he served on the President's Council of Advisors of Science and Technology advisory group that examined ways to transition federal spectrum for commercial use. Dr. Reed is a past member CSMAC a group that provides advice to the NTIA on spectrum issues and has testified before Congress on the need to support research in spectrum issue.

SWARMSENSE: EFFECTIVE AND RESILIENT DRONE SWARM AND SEARCH FOR DISASTER RESPONSE AND MANAGEMENT APPLICATION

Bo Ryu (EpiSys Science, USA); Cheolmin Jeon, Jeongsoo Ha, Hanbum Ko and Byeongman Lee (EpiSys Science, Korea)

Speaker Biography
Hanbum Ko

- B.S. Computer Science & Engineering, Statistics
- Chungnam National University
- AI/ML Research Intern at EpiSci (EpiSys Science, Inc.)
- Hanbum Ko is a senior studying Computer Science and Statistics at Chungnam National University in Daejeon, Korea. His interests lie in the areas of advancing computer vision and multi-agent reinforcement learning. Currently an artificial intelligence and machine learning research intern at EpiSci, Hanbum is developing computer vision algorithms for SwarmSense, a modular UAV swarm system that enables efficient and effective multi-drone operations. He can be contacted at hanbum@episyscience.com

Speaker Biography
Cheolmin Jeon

- B.S. Computer Science & Engineering,
- Chungnam National University
- AI/ML Research Intern at EpiSys Science, Inc.
- Cheolmin Jeon is a fourth year Computer Science undergraduate student from Chungnam National University. He began his artificial intelligence and machine learning research internship at EpiSci (EpiSys Science) in March 2019 and participated in AFRL's Swarm and Search AI challenge. An innovative and creative thinker, he is currently researching and implementing autonomous, dynamic, and collaborative wireless communication algorithms into EpiSci's drone swarm solution, SwarmSense. He can be contacted at cheolmin@episyscience.com