A Review on Cybersecurity Vulnerabilities for Urban Air Mobility

Anthony C.B. Tang[1]
National Aeronautics and Space Administration

Recent developments of high-powered unmanned aerial vehicles (UAVs) have allowed for urban air mobility (UAM) to become a reality. While these flying cars' propulsive technology has almost become economically viable, the infrastructure to allow these vehicles to operate in an urban environment is still lacking. With numerous known vulnerabilities in UAVs and commercial aircraft, manufacturers have not addressed cybersecurity in the scope of urban air mobility. This paper presents a review of several known cybersecurity vulnerabilities and previous attacks associated with UAVs and aircraft's core communication systems. Analyzing current solutions to each threat and incorporating early concepts for UAM, this paper then presents a basic cybersecurity framework featuring a blockchain-based PKI with secondary navigation systems to allow for the development of secure airspace.

I. Introduction

Urban air mobility (UAM), revolving around the decades-old dream of flying cars, is now positioned to revolutionize the transportation industry. Relying on high-powered unmanned aerial vehicles (UAVs) to act as flying cars for passengers, UAM is a subset of Advanced Air Mobility (AAM), an initiative led by the National Aeronautics and Space Administration (NASA), the Federal Aviation Administration (FAA), and industries to develop a next generation air transportation system for people and cargo. To allow for this development, government agencies, such as NASA and the FAA, are in the process of developing the necessary infrastructure for future integration of UAVs into the national airspace system (NAS). In 2016, the FAA first set basic guidelines for small unmanned aircraft under 55lbs [1]. Pushing the development, the FAA in 2019 proposed policies regarding remote frequency identification (RFID) [1, 2]. Most recently, in 2020, the FAA released its early thoughts on UAM in its *Version 1.0 of the Urban Air Mobility (UAM) Concept of Operations* [3]. Many other large corporations and NASA have already identified different concepts and considerations for UAM [4-6]. Although rules and regulations are progressing, there still is a glaring need to address cybersecurity within the scope UAM to provide a secure airspace.

This paper condenses and reviews several scientific journals, reported vulnerabilities, reported attacks, concerns, and possible solutions for UAVs in the context of UAM. UAVs for UAM have aspects in common with small UAVs, large UAVs, and commercial aircraft. Thus, this paper reports all known relevant vulnerabilities of all three types of aircraft. For this paper, a small UAV, such as the DJI Phantom, is defined as under 55 lbs. A large UAV, such as the General Atomics MQ-1 Predator, is defined as over 55 lbs. The terms "drone" and "UAV" are considered synonymous. A commercial aircraft refers explicitly to any in-person manually operated aircraft such as a Boeing 737, and both commercial aircraft and drones are types of aircraft. A "flying car" or "flying vehicle" explicitly refers to a UAV for UAM that is manufactured to transport human passengers.

The need to assess all three types of aircraft is due to the expectation that flying cars will operate within urban environments such as San Francisco or New York while flying at altitudes up to a few thousand feet [6]. Due to the nature of carrying passengers, industry initiatives and experts expect flying cars to obey similar safety standards of commercial aircraft [4, 6]. Simultaneously, flying cars are expected to be remotely controlled and tracked similarly to small and large UAVs [4].

This paper first outlines all known cybersecurity incidents and vulnerabilities relevant to existing UAVs and commercial aircraft. Next, the article assesses current solutions to the known cybersecurity vulnerabilities. Finally, this paper analyzes the feasibility of all solutions in the scope of UAM and proposes an overall necessary infrastructure to ensure proper safe cybersecurity operations for future flying cars.

[1] Student Intern, Secure Airspace, Ames Research Center Aeronautics Projects Office.

II. Background

This section outlines the different communication systems of a flying car that are in common with UAVs or commercial aircraft. Each system poses cybersecurity risks for the potential for unauthorized users to remotely obtain information or gain control of the aircraft with malicious intent. Each risk may be identified after a deliberate attack or through a simulated attack meant for demonstration purposes, and they may be associated with one or more communication systems. For the scope of this paper, cybersecurity risks involve only the data transmission through data links between different digital parties, and this paper does not consider physical security. Figures 1 and 2 below illustrate the conventional telemetry comprised of UAVs and commercial aircraft's core systems with each respectful data link. All vertical lines between systems represent an electromagnetic-based communication link, while horizontal lines between systems represent integrated wired connections within an aircraft. In addition, systems that may be combined into a single data link are outlined with a dotted box, and their resulting connections are also dotted.

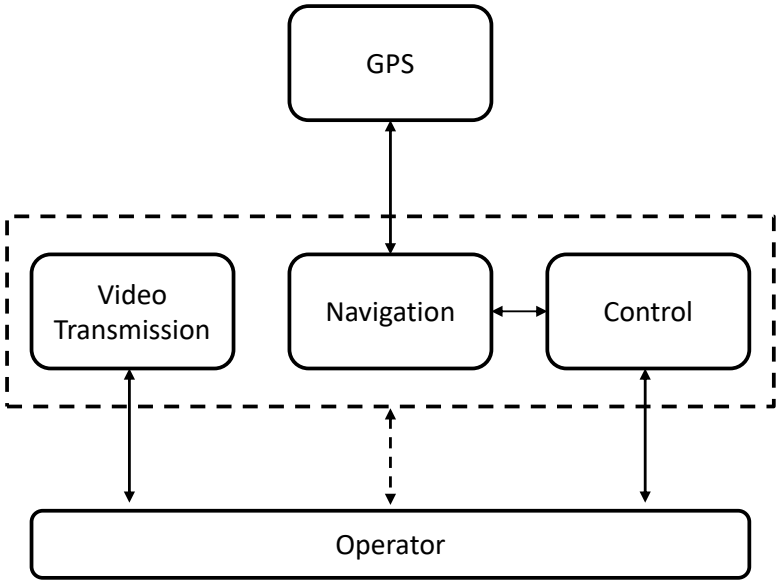

Figure 1. Telemetry and Data Links of UAVs

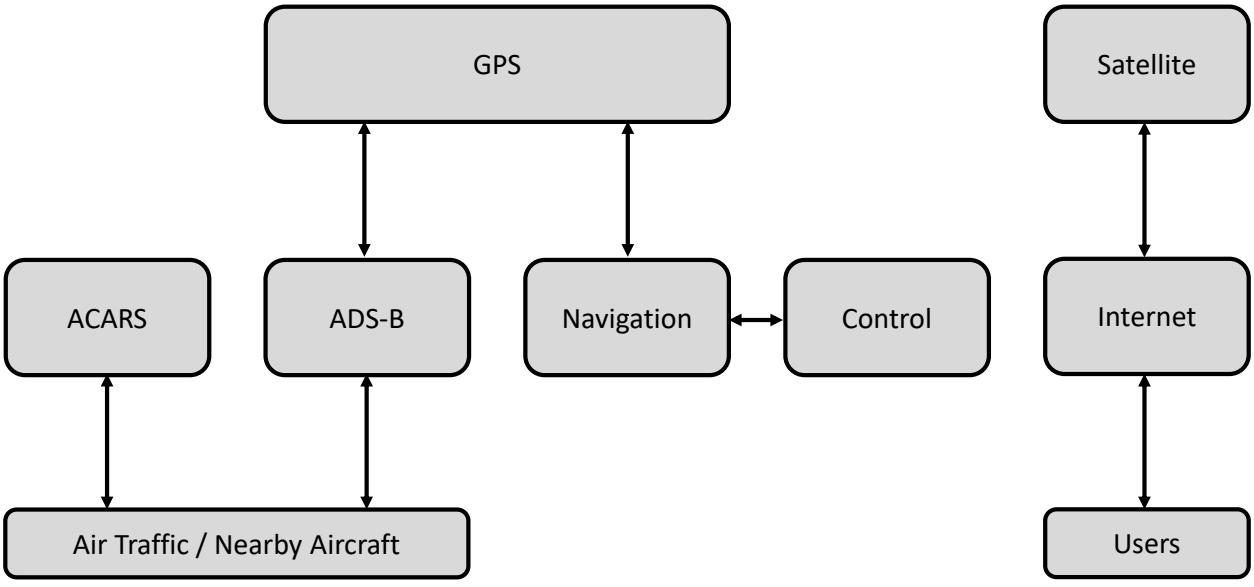

Figure 2. Telemetry and Data Links of Commercial Aircraft

A. Control, Video Transmission, and Navigation

There are many different communication links and possible configurations for an aircraft's controls and video transmissions. UAVs primarily use a 2.4GHz or 5.8GHz radio frequency (RF) connection for their control and video transmission links [7]. For small and large UAVs, these connections often serve as a manual control link between a physical remote controller and the UAV, an automated control link between a remote computer and the UAV, or a video transmission link between an on-board camera and a computer. Remote controllers and remote computers are assumed to be controlled by an operator. For some large UAVs that operate beyond-line-of-sight (BLOS), a tertiary satellite connection offers an additional control link to the operator. Since commercial aircraft usually are neither remotely controlled nor transmitting video feeds, control and video transmission data links are not relevant. However, a 2.4 GHz or 5.8 GHz connection may be present on commercial aircraft for in-flight wireless internet connections.

Basic small UAV systems involve a UAV with a pre-installed identification system paired to the remote control (RC) controller for an operator to securely control the UAV. Like wireless car keys, the exact method to secure the link between the UAV and RC controller is often proprietary and will differ between manufacturers. Thus, a controller for one drone will usually not work with another drone from a different manufacturer. The UAV operator can receive video feed and images from an on-board camera through a wireless connection. For basic small UAVs, the controls and video transmission links may operate either:

1. Independently on the same frequency
2. Independently on different frequencies
3. Jointly on the same frequency through a combined data link

Many small hobbyist UAVs have configuration (1) or (2), with some preferring configuration (2) over (1) because of its higher bandwidth. In configuration (3), the UAV often uses an on-board computer that combines the control and video transmission data links. This on-board computer with specialized software connects to the operator through a direct line-of-sight (LOS) wireless connection or BLOS satellite connection. A user can then control the UAV while simultaneously receiving video transmission through this application. Advanced drones often have configuration (3) to allow for autonomous flight mapping and other automated features. However, these advanced drones with autonomous flight mapping usually contain an independent manual control data link in case of an emergency.

In all configurations for UAVs, the securing of the data links depends on the manufacturer and specific product. When control and video transmission are independent, almost all manufacturers secure the control data link, including BLOS connections, through encryption or radio frequency identification (RFID, but some leave the video transmission unencrypted. When the two data links are combined, some manufacturers establish and protect the resulting link through WPA2 Wi-Fi connections or IP tunneling protocol. However, the final architecture widely differs among manufacturers. All civilian GPS connections are currently not encrypted.

For positioning and navigation information to aid the control links, some drones and all commercial aircraft have an accurate global position system (GPS) that connects to a geosynchronous satellite [8]. Some large UAVs and most commercial aircraft also are equipped with an inertial navigation system (INS) that serves as a backup to the GPS. Since these systems rely on a non-digital signal transmission or a signal between a physical object and a signal transmitter, they are also not considered data links.

B. Management and Surveillance Communication

To maintain the safety of the NAS, the FAA has established systems to manage and monitor commercial aircraft, and the FAA is currently in the process of establishing similar systems to manage and monitor UAVs that operate within the NAS. These unfolding policies for UAVs are referenced in the FAA's *Version 1.0 of the Urban Air Mobility (UAM) Concept of Operations*, and it is essential to outline the existing policies for commercial aircraft and unfolding policies for UAVs in the scope of UAM.

1. Communications Addressing and Reporting System (ACARS)

For commercial aircraft, the established systems to manage and monitor aircraft involve the Aircraft Communications Addressing and Reporting System (ACARS) and the automatic dependent surveillance-broadcast (ADS-B) system. The ACARS is a communication data link between aircraft and ground stations via very high frequency (VHF) radio, high frequency (HF) radio, or satellite communication (SATCOM) [9]. Between aircraft and ground stations, ACARS messages may generally be categorized to serve one of three purposes:

- Air Traffic Control communication for operations such as clearance for take-off or landing
- Aeronautics Operational Control communication for weather reports, flight plan changes, or emergencies

- Airline Administration Control communication for airline-specific communication [10]

The ACARS messages are sent using a Communication Management Unit (CMU), which functions as a router that connects to VHF stations through LOS, HF stations through LOS, or SATCOM stations through satellite connections. ACARS messages can be sent either in clear text or encrypted.

Since aviation movements through communication, including ACARS, eventually allow third-party organizations such as Flightradar24 and FlightAware to publicly display an aircraft's position and route, some aircraft seek privacy through the National Business Aviation Association's Blocked Aircraft Registration Request (BARR) [11]. This program helps airlines and aircraft owners prevent their data from becoming publically known. However, while a blocked aircraft helps prevent the spread of information to the public, a blocked aircraft does not prevent an attacker from intercepting ACARS messages themselves. As a result, even on the block list and with encryption, the ACARS system has been a point of cybersecurity concern due to its possibility to allow an attacker to obtain financial or operational data, sensitive flight plans, or more detailed information about flight status.

2. Automatic Dependent Surveillance-Broadcast (ADS-B)

While ACARS can be seen as a direct communication method between aircraft and ground stations, the ADS-B is an automatic broadcasting of information to help maintain the organization and supervision of the national airspace. Found in all commercial aircraft and many helicopters, ADS-B currently is a well-established surveillance technology that broadcasts an aircraft's vital information, including position, velocity, and altitude for air traffic management (ATM) and other aircraft [12]. Similar to any communication system, there is an ADS-B Out transmitter and an ADS-B In receiver. As of January 1st, 2020, the ADS-B Out transmitter is required for any aircraft that flies in class A airspace or above 18,000ft. A GPS connection or another certified global navigation satellite system (GNSS) provides the information of the aircraft to the ADS-B Out transmission. Anyone with an ADS-B In receiver can receive the transmitted signals of the ADS-B Out [13]. While the information of the ADS-B allows for active tracking and management of all nearby planes that eventually lead to public dissemination, security researchers have raised concerns because the data is neither encrypted nor authenticated [12]. Similar to ACARS, some experts have long identified the ADS-B as a security risk since the currently available information could reveal sensitive, valuable financial data of commercial airfare and classified aircraft position data of military airfare [14, 15]. In 2019, the FAA revised their ADS-B Out requirement for military aircraft by now allowing them to turn off the transmitter during sensitive operations [16]. Due to the unauthenticated nature of ADS-B, ADS-B can also easily be spoofed.

3. Radio Frequency Identification

Radio frequency identification, or RFID, is emerging as a likely method to track and monitor UAVs in a nearly identical manner as ADS-B. While these two systems are not mutually exclusive, it is crucial to outline the current unfolding expectations of the two within the scope of UAM. A developing system for UAV management, RFID can also broadcast an unmanned aerial system's vital information such as identification, position, velocity, and altitude for air traffic management. RFID acts similarly to a radio barcode such that a reader can identify an object when requested. Thus, ADS-B and RFID are both key aspects of aircraft management and surveillance [17].

In 2019, the FAA proposed mandating RFID on all unmanned aircraft systems with only a few exceptions that include military aircraft and UAVs under 0.55lbs. Specifically, this proposal looks to mandate equipment that broadcasts the identification information of an aircraft in addition to flight information like the ADS-B. These rules are built on the FAA's 2015 rules that require all UAVs above 0.55lbs to register with the FAA and display identification information. These 2015 rules called for the physically labeled unique serial number on the aircraft and the UAV model and ownership registration. Before 2019, the unique UAV serial number was only validated through physical examination of the aircraft; thus, the 2019 proposal would allow law enforcement to remotely validate this information to create an ADS-B-like remote infrastructure for small and large UAVs.

The FAA expands on this ADS-B-like remote infrastructure using RFID in their *Version 1.0 of the Urban Air Mobility (UAM) Concept of Operations*. In it, the FAA presents the concept of flying vehicles operating within designated corridors that feature these important principles:

- All aircraft operate under UAM specific rules, procedures, and performance requirements
- Fixed-wing aircraft and other UAV aircraft cross UAM corridors
- Helicopters and UAM aircraft operate within or cross UAM corridors
- Operations do not vary within airspace class [3]

However, outside of UAM corridors, "operations adhere to relevant ATM and UTM (unmanned aerial systems traffic management) rules based on operation type airspace class, and altitude" [3]. These new principles outline the creation of a new airspace structure that would allow flying cars to operate within the NAS while working somewhat independently from the existing airspace that is currently well-established for only commercial aircraft. Figure 2 below illustrates the proposed corridor system to enable safe operations for UAM.

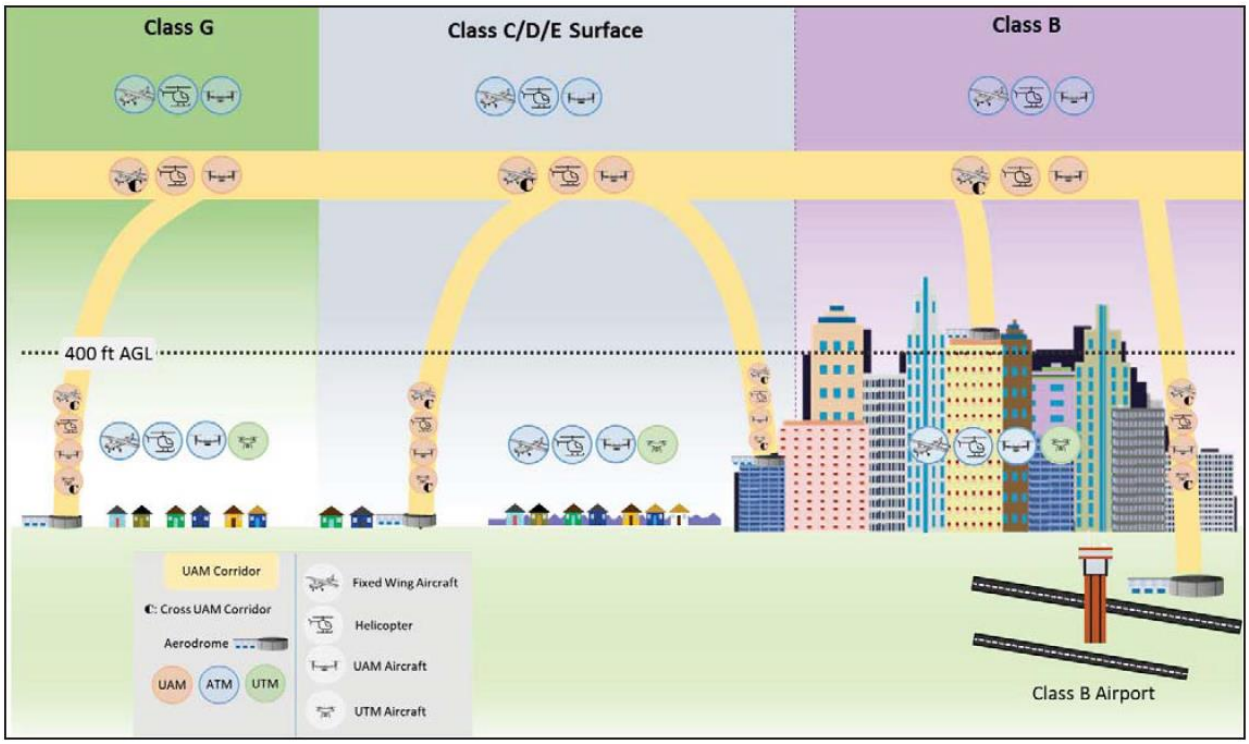

Figure 2. The FAA's Proposed UAM Concept of Operation [3]

The new proposed NAS structure also strives to minimize disruption on the pre-existing conditions for commercial aircraft. Most notably, the FAA notes that they assume UAM aircraft will offer identification and location information, but "not provided by ADS-B Out or transponders for operations in the UAM Corridor(s); however, other functionality (e.g., UAM applicable Remote ID) may support this identification and location information capability." Combined with the mentioned principles, it can be inferred that the FAA hopes to minimize any disruptions to the already used ADS-B frequencies. Ultimately, the FAA is hoping flying cars can use RFID for management and surveillance within the UAM corridors. However, flying cars will still need to have an ADS-B system in the unexpected case that the aircraft needs to leave the corridor.

C. Internet Connectivity

The most significant component in the modern digital era, the internet, is a necessity for some users, and the internet is present in some commercial UAVs and many commercial aircraft. For UAVs, an internet connection through a "home station" allows for cloud connectivity as a means for multi-element connectivity and storage. The data transfer is often through IP tunneling. These systems require an on-board computer that often uses a combined data link that allows for more advanced data processing and communication. Many researchers have proposed several different systems of UAVs that can operate within normal Wi-Fi ranges, and smaller UAVs are already integrated with other Internet of Things (IoT) devices [18]. These IoT devise can connect to online services, which provides new means for attackers to compromise the system.

For commercial aircraft, an internet connection through satellite connections allows users to use the web as they fly in the sky, outside of any cellular network. Satellite internet service providers like Gogo Incorporated have satellite agreements with satellite owners such as Intelsat and SES S.A., and the airliners pay for the data [19]. Since this connection is governed by the satellite internet provider and the satellite owner, securing the internet data link is at the discretion of these companies.

III. Cyber Attacks and Recent Incidents

This section outlines the different possible cybersecurity attacks involved with the various data links of aircraft. Physical drone attacks not tied to cybersecurity, such as a drone physically flying into protected airport airspace under the direction of a malicious or simply unskilled pilot, are not considered. Also, this section presents recent incidents or demonstrations of each attack. Each possible attack relates to one or more of the data links.

D. Jamming

All data links are vulnerable to one of the most elementary and frequent cybersecurity attacks - jamming [20]. Jamming involves using a device to interrupt a targeted RF signal physically [21]. Several companies have already developed anti-drone equipment to take down UAVs or render them uncontrollable through jamming [22]. However, manufacturers have been aware of jamming for many years, and many manufacturers have developed measures in place in the case that the control data link is jammed or lost. For example, the DJI Phantom 4 has an on-board computer with a "Failsafe" feature that will cause the drone to either hover in place, return to a pre-determined home location, or automatically land in the case of a lost connection that may be the result of jamming.

However, this basic level of control and software backup still may pose a threat, as seen in an incident with an MQ-8B Fire Scout UAV in August of 2010. What investigators later called a "software issue," the 1,429 kg UAV lost connection with its human operators for approximately 30 minutes [23]. In this time, the drone drifted into a heavily regulated airspace of the Andrews Air Force Base after it failed to execute the software commands that would have forced it to return to base. While this incident is not from deliberate jamming, the effects are still the same, and in this incident, the safety measures in place failed to remedy the situation.

In May 2012, another jamming incident took place in South Korea when a 150 kg Schiebel Camcopter S-100 drone crashed into its ground-control station, killing an engineer while injuring others [24]. In this case, attackers believed to be from North Korea jammed the drone's GPS, causing difficulty of controls. South Korean authorities confirmed the GPS jamming attacks [25].

E. Spoofing

Spoofing is an attack in which a nearby radio transmitter sends illegitimate information, such as wrong GPS coordinates, to the receiver to trick it. Spoofing is prevalent in GPS connections and can be associated with ADS-B, internet, and other navigation connections. Often associated with GPS jamming, GPS spoofing has caused many cybersecurity issues for UAVs since many rely on the information to navigate. Although not exclusive to the GPS, spoofing can easily take advantage of a UAV's built-in stabilization system or autonomous flight plan by giving it the impression it is at an undesired location or traveling in an undesired direction that it then must correct.

In arguably the most alarming UAV cybersecurity attack, a large fixed-wing Lockheed Martin RQ-170 UAV was captured by Iranian forces in 2011 due to a satellite jamming and spoofing attack [26, 27]. According to an Iranian engineer, Iranian forces first jammed the satellite control signals, then conducted a GPS spoofing attack to land the UAV in a location it was not supposed to land. Thus, this attack took advantage of software like DJI's "Failsafe" program that uses GPS information to land the UAV, where it believes it initially took flight.

Several other sophisticated GPS spoofing attacks have been demonstrated and simulated. In 2012, the University of Texas Radionavigation Laboratory commanded an $80,000 Hornet Mini rotorcraft by Adaptive Flight, used by law enforcement, to suddenly dive to the ground by inducing a false upward drift through GPS spoofing [28, 29]. This sophisticated drone touted inertial sensors such as accelerometers and altimeters. However, this demonstration for the Department of Homeland Security (DHS) sheds light on the continued insecurity of GPS signals even when equipped with secondary and tertiary control and navigation systems.

Other GPS spoofing demonstrations include the Parrot A.R 2.0, a more hobbyist UAV with known zero-day vulnerabilities. A zero-day vulnerability is simply a known software security flaw that is not fixed. Some of these flaws include vulnerable ports, weak processing units, and vulnerable access points [30]. In the case of GPS spoofing, researchers have demonstrated landing a Parrot A.R 2.0 at an incorrect location through GPS spoofing to further demonstrate UAVs' vulnerabilities, given that the position and intended travel path is known [29]. This demonstration highlighted the Parrot A.R 2.0’s command to navigate in the direction of its destination relative to its current position. If a Parrot A.R 2.0’s current position is spoofed to be south of its intended destination, the UAV believes its destination is north of it. In actuality, its destination may be elsewhere of the UAV; thus, the UAV travels in the wrong direction.

F. Man-in-the-Middle (MITM)

Frequently seen in movies, MITM and interception attacks have been well hypothesized and demonstrated for UAVs. For the scope of this paper, a problematic MITM attack for a UAV can refer to an unauthorized user intercepting and manipulating video transmission from a UAV in a replay attack. If an operator controls the UAV through a first-person view (FPV), a MITM attack can directly cause the UAV to crash. A MITM attack can also refer to unauthorized users eavesdropping flight directions/conversations or intercepting video feed. While eavesdropping attacks may not give control of an aircraft, the data in the live-streamed video transmission can be vital information for surveillance purposes. In both cases, the host may never be aware of the breach.

While there have not been any reported MITM attacks on a large drone that compromises the controls and operations, researchers have demonstrated MITM attacks on small drones with Wi-Fi connections for controls and video transmission. In 2016, a researcher demonstrated how to compromise the wireless Parrot A.R 2.0 at Black Hat Asia [31]. Highlighting the hackable wireless connection, the researcher executed a MITM attack to read, send, and alter the data stream between the UAV and wireless host that controls the UAV.

G. Denial of Service (DOS)

Just as any computer with a wireless connection is vulnerable to a DOS attack, many UAVs are also susceptible to similar attacks. Depending on the type of communication link that uses the wireless connection, a DOS attack can undermine a UAV's controls or video transmission. There are many types of DOS attacks with consequences ranging from a full takeover of the UAV to rendering the UAV vulnerable to a follow-up attack.

In 2013, Samy Kamkar, a well-known hacker and cybersecurity expert, uncovered a program he developed that uses a deauthentification DOS attack to wirelessly hack and take over any Parrot A.R Drone [32]. Using only Kali Linux, basic electronics found on Amazon, and the program he called "SkyJack," Kamkar was able to fully take control of the UAV's controls and video transmission that takes place through a single data link [33, 34]. Specifically, Kamkar used his program to disconnect the wireless connection between the true owner and drone, then authenticate himself with the target drone pretending to be its owner, ultimately gaining complete control of all the data links, including controls and video transmission [32]. Parrot has since discontinued the A.R Drone series, but similar deauthentication attacks can still be applied to any UAV assuming the Wi-Fi connection is hackable.

Further highlighting the security flaws of small UAVs, security informatics graduate students at John Hopkins discovered three security flaws in a popular hobby drone in 2016 [35]. The first security flaw involved bombarding the UAV with wireless connection requests to overload the UAV's central processing unit, causing it to shut down and fall out of the sky. The second vulnerability was also traced to the central processing unit after the team sent an exceptionally large data packet and overloaded the flight application. The final vulnerability was a deauthentication attack. All of the types of DOS attacks rendered the UAV useless momentarily and resulted in an "uncontrolled landing."

H. Internet Connectivity

For UAVs, an internet connection often allows for cloud connectivity as a means for data connectivity and storage. For commercial aircraft, an internet connection allows for users to use the web as they are flying, outside of any cellular network. As a result, internet connectivity has opened new means for attackers to compromise an aircraft.

There are no known incidents of a UAV system becoming compromised because of an internet connection. However, deploying drones through cloud connectivity and cloud connection is a rapidly emerging research area analogous to several other robotic applications [36-39]. In everyday homes, Internet of Things (IoT) devices with internet connections include smart TVs, smart refrigerators, wireless security cameras, and much more. Wireless security cameras may serve as an excellent example of an often cloud-based service that hackers have compromised numerous times. In 2019, a hacker gained access to a family's Ring security camera and was able to talk through the system [40]. In 2017, London authorities arrested two suspected hackers on suspicion of hacking 70% of CCTV cameras in Washington, D.C., just days before President Trump's inauguration [41]. In the former case, the cause was due to a compromised personal password, and the latter case was due to ransomware. Both scenarios highlight a widened possibility of cybersecurity vulnerabilities that is characteristic of any IoT device.

Of commercial aircraft, there have been reports of hacking into commercial planes such as the Boeing 757. In 2017, a Department of Homeland Security (DHS) official admitted that he "was successful in accomplishing a remote, non-cooperative, penetration" and that his team of experts was able to "establish a presence on the systems of the aircraft" [42]. While the DHS never released the details of this compromise, in-flight internet providers themselves have advised users not to access sensitive information on flight, possibly because of its lack of security [43]. In 2013, a cybersecurity researcher, Ruben Santamarta, identified numerous security vulnerabilities in different types of satellite communication (SATCOM) that helped to provide internet for aircraft [44]. The vulnerabilities included

backdoors, weak password resets, and insecure protocols. Since then, many airliners and manufacturers of satellite systems have claimed to have addressed these vulnerabilities [45]. Santamarta has continued to publish aviation cybersecurity vulnerabilities. While he has stated that there is no immediate flight risk, he identifies internet connections as an aviation risk that allows for the following:

- ability to disrupt, intercept or modify non-safety communications such as Wi-Fi
- ability to attack crew and passenger's devices
- ability to manipulate SATCOM antenna positioning and transmissions [46]

Most importantly, Santamarta and other cybersecurity experts have pointed out that to maintain the aircraft's safety, non-essential communications such as Wi-Fi internet connections must be strictly separate from the controls and the vital avionics [42].

I. ADS-B

Due to ADS-B's unencrypted and authenticated nature, the possible threats include all the previously mentioned vulnerabilities, including jamming, denial of service, eavesdropping, spoofing, message injection, and message manipulation [47]. In just one example, security researcher Brad Haines publicly demonstrated an ADS-B spoofing attack by inserting a fake aircraft into a simulation of San Francisco's airspace in 2012 at the DEF CON20 security conference [48]. Researchers Andrei Costin and Aurelian Francillon have confirmed that this type of spoofing attack is not only possible but "easy and practically feasible, for a moderately sophisticated attacker" [47]. Currently, several websites such as ADS-B Exchange openly display flight information of aircraft across the globe from hobbyist-owned ADS-B. The FAA has stated that they are aware of the issues and risks of ADS-B. However, they have not publicly announced any efforts of encryption or authentication [49].

J. RFID

There have not been any RFID cybersecurity incidents on UAVs and aircraft, mostly because RFID technology is still in its infancy for UAV applications. However, RFID technology, including credit cards, has been long researched as a possible cybersecurity threat when the ID tags contain sensitive information [50]. Since the FAA is positioning RFID to serve as a new-and-improved ADS-B, the sensitivity of the information on a UAV's RFID can be assumed to be analogous to ADS-B. However, since RFID is still in development, there likely will be many options for UAV developers to employ an RFID system with encryption and authentication, thus adding significantly more cybersecurity.

K. Summary of Known Vulnerabilities

Currently, there are several cybersecurity risks to both small and large UAVs and commercial aircraft. These cybersecurity risks involve several different components of a UAV or a commercial aircraft such as the control data link, GPS connection, on-board computing systems, or ADS-B broadcasting system. In summary, the different attacks that a UAV or commercial aircraft may be vulnerable to includes:

- RF Jamming
- Spoofing
- Man-in-the-Middle
- Deauthentication
- Eavesdropping
- Injection
- DOS

Through demonstrations or real experiences, these attacks can fully compromise the integrity of a UAM system, and it is necessary to address these vulnerabilities to create a secure airspace.

IV. Existing Solutions

As the world has become more digitized, cybersecurity experts and engineers alike have proposed numerous solutions to the cybersecurity vulnerabilities mentioned. Proposed solutions are into two categories: direct prevention and secondary systems. While the goal of direct prevention is preventing a compromise, secondary systems may work to identify a compromise, authenticate information, or serve as a backup system in the case of failure. Direct prevention is more relevant for UAV video feed transmission and management systems. Secondary systems are more relevant for UAV command and navigation.

A. Direct Prevention

1. Spread Spectrum and Jamming Detection

Jamming is a physical interference of radio frequencies, and researchers have categorized jammers into four different categories: constant, reactive, deceptive, and random [51]. Traditional physical layer solutions to prevent jamming attacks include a type of spread-spectrum (SS) technology where the communication takes place over multiple frequencies. In methods such as the FCC approved frequency-hopping spread spectrum (FHSS) method, the carrier frequency changes rapidly within a known broad spectral band [52]. Only the authorized transmitter and receiver should know the exact changes and thus means to interpret or jam the signals. However, while the signals may be highly resistant to narrowband interference and signal interpretation without knowing the hopping pattern, wideband interference that can cover all the frequencies may still pose a threat given a potent enough jammer. Other similar modes of SS include the direct sequence spread spectrum and uncoordinated spread spectrum.

While the U.S has widely adopted many forms of SS for different communication systems, the means of detecting jamming is also vital to allow for secondary systems to support an operation. The most popular method to detect jamming or any interference, including spoofing, is through statistical analysis methods. The several different ways to statistically detect a jamming signal is out of the scope of this paper, but some of them include analyzing the signal strengths, the consistency of signal strengths, carrier sensing time, and packet delivery ratio. Most of those methods involve building a statistical model of different characteristics of the RF signal under controlled operations without jamming to detect and filter out jamming efforts that may happen during service [51]. Once statisticians develop these models, on-board aircraft computers can detect jamming if their received RF signals do not fit the model. In this case, the aircraft will then follow a specified protocol that may involve a secondary system to allow the aircraft to continue operating in the jammed area.

2. Standard Encryption

Encryption has emerged as one of the essential cybersecurity tools to protect sensitive data for all types of digital communication. Standard encryption can potentially prevent a wide range of DOS attacks, spoofing attacks, eavesdropping, and injection attacks for several different data links, including navigation/control, video transmission, and ADS-B. While there are several different types of encryption, encryption is generally a process in which a transmitting party converts a digital message into an alternative and unreadable form using a unique mathematical algorithm before sending it. The algorithm uses secret keys that act like passwords, and only those parties with the appropriate keys can decrypt and understand the message. Ultimately, encryption ensures that communication is only between approved parties. However, an essential issue for encryption protocols is the insurance that each key is authentic. Thus, there is often a need for third parties – known as certificate authorities (CAs) – to certify the ownership of critical pairs. The distribution and system of keys using CAs are known as public key infrastructure (PKI), and there are other crypto-infrastructures.

Applicable to the control link, video transmission link, ADS-B, and internet connectivity, there are two different types of encryption: symmetric and asymmetric. The Advanced Encryption Standard (AES) encryption is an example of symmetric encryption, and the Rivest-Shamir-Adleman (RSA) encryption is an example of asymmetric encryption [53]. AES, which is the current standard for encryption, has been widely adopted by the U.S government and is now used worldwide. AES relies on using the same key for both encrypting and decrypting the data [54]. On the other hand, RSA encryption is an asymmetric key system that uses a shared public key to encrypt data and unique private keys to decrypt the data [55]. There are many other symmetric and asymmetric encryption methods, but the two crucial differences between the two types are the key management required and the performance tradeoffs.

Key management involves the handling of keys that can undermine the security of an overall encryption scheme. With symmetric-key encryption, the same key is used to encrypt and decrypt the data sent, but this means that compromising a single key can undermine an entire system. If encryption is between several elements, an attacker with a single compromised symmetric-key can read and send information between other devices relying on the encryption. In a symmetric-key system with few elements, the keys can be more easily protected and monitored while

jeopardizing only a few elements. In an extensive multi-element system, the numerous keys can be difficult to secure and monitor, and a single compromise can mean a catastrophe as all the elements are now compromise [56]. There are two different types of keys in asymmetric key encryption – public keys, which CAs distribute freely, and private keys, which are usually kept extremely secret. The resulting communication is more one-way because while the distributed public keys may mean that several parties have the means to encrypt the data, only private key holders can decrypt the data, or vice versa. In this case, if a public key is compromised, then only the link between the private key is compromised, but not other public keys. While this may put more significant stress on the private key, it is often still easier to focus on protecting a few important private keys [57] rather than several symmetric keys.

Performance tradeoffs are a vital aspect to consider in determining the best encryption scheme. AES not only has been noted to have strong security, but also high speed. Specifically, AES encryption's hardware and software implementation are exceptionally fast since parties use only a single key to encrypt and decrypt information. In comparison, the public key encryption of RSA encryption is significantly more computationally intensive. Ultimately, some studies have found that asymmetric encryption techniques can be up to 1000 times slower than symmetric methods due to the more massive required processing power [58]. While this metric can be deceiving due to the dependency on processing power and packet size, a study has found that it takes approximately 3 to 4 times longer to encrypt and decrypt an 868kB package using RSA encryption compared to AES encryption [55]. If an encryption scheme's required computational demand adds significant latency to a UAV's on-board processing, that type of encryption may not be viable. While this may not be the case, in reality, there are several proposed modified asymmetric and symmetric encryption schemes, including lightweight versions. Regardless, the two systems' successful key management's general performance tradeoffs and requirements remain the same.

3. GPS Encryption

Currently, GPS connections for all civilian uses are unencrypted. Unlike simple radio connections, encryption of GPS connectivity is usually not feasible because the U.S government solely manages the GPS satellite array. As a result, any current receiver can receive a spoofed GPS signal and fall victim to an attack. However, encrypted GPS signals and anti-spoofing measures for GPS receivers exist, but the U.S government has reserved these methods for military operations only [59]. Either P(Y) code or M-Code, encrypted GPS signals exist on the same frequency as standard GPS signals, and much of the information about the algorithms and means of decrypting these signals are publicly unknown. P(Y) code involves the combination of a public code that allows for more exact coordinate information, and a cryptographically generated Y-code created through an anti-spoofing module [59]. The classified M-code is autonomous and of an unknown length and nature. Currently, the only method to secure aircraft navigation systems is with secondary systems to authenticate GPS signals.

4. Blockchain

While not wholly different from encryption, blockchain has emerged over the past years as an innovative approach in organizing a digital multi-element system. A decentralized system, blockchain links multiple subsystems, known as blocks, through cryptography that, by design, is resistant to modification of data [60]. Since blockchain is a means of securely recording different transactions, blockchain offers a digital infrastructure for countless applications, including financial institutions, supply chain management, voting, and air traffic management [61]. However, since blockchain is a new method to organize and track transactions in a multi-element system, a major hurdle of blockchain is implementing it in a pre-existing system. Yet, for emerging or not yet established digital ecosystems, such as air traffic management for flying cars, blockchain has seen a surge in interest because it can help manage encryption of control, video transmission, ADS-B, RFID, and other systems.

Addressing the ADS-B concern, NASA engineer Ronald Reisman presented a novel blockchain-based PKI for aviation surveillance applications in 2019 [62]. Acknowledging the absence of any approved efforts to harden the ADS-B system, Reisman proposes using the open-source blockchain platform "Hyperledger Fabric" that developers designed explicitly for enterprise transactions that resemble typical air traffic management interactions. Reisman highlights the use of private channels to communicate sensitive information at relatively high bandwidth, thus allowing ADS-B users to maintain their privacy from the public while still communicating with essential authorized parties. Incorporating encryption, Hyperledger Fabric also provides a standardized PKI infrastructure with CA features to ensure identity authentication and authorization of the keys for authorized parties.

B. Secondary Systems

Secondary systems are essential for supporting or authenticating primary control/navigation systems. For this paper, emergency software protocols like the DJI's "Failsafe" mode are not secondary systems. These software protocols are often part of the integrated computer and cannot be a standalone system if necessary. Since control

systems and management systems are heavily dependent on the navigation system for autonomous flight execution and remote control, secondary systems are critical for navigation systems. Consequently, secondary systems provide the necessary redundancy and constant validation to support the controls and primary navigation data link as jamming and spoofing attacks threaten its integrity. Currently, the most precise and widely used method to obtain navigation information is through GPS, and the numerous technologies outlined in this section can replace or support GPS in a spoofing or jamming attack. However, GPS still touts the most exceptional accuracy of all navigation systems. Thus, it is best to use secondary systems only to validate GPS positioning and in an emergency.

1. Inertial Navigation System (INS)

An inertial navigation system (INS) is a processing unit that uses only on-board motion sensors to calculate a body's physical characteristics like location, orientation, and velocity. Containing inertial measurement units (IMUs), an INS relies on accelerometers, gyroscopes, and other tools to obtain information about the moving body without any external reference. As a result, INS is immune to jamming and spoofing.

While INS theoretically can be a primary navigation system, it is primarily a secondary system to validate the more precise GPS signal continually. INS is not ideal for primary navigation systems because it suffers from integration drift: small errors in the calculation of acceleration and velocity that compound to greater errors in position. As a result, inertial navigation works best when frequently recalibrated by confirming inertial values by stopping at a known location or when a given velocity or acceleration is guaranteed [63]. Ultimately, INS provides a means for GPS validation but offers a reliable backup navigation system if there is GPS jamming or spoofing. Many combat-ready UAVs contain at least an inertial navigation system alongside GPS connectivity, and other navigation systems can help correct the errors due to INS drift.

2. . Celestial Navigation System

Using celestial bodies such as the sun and moon as reference points, celestial navigation is another standard method for an aircraft or naval vehicle to determine its location. Celestial navigation relies on the use of angular measurements between celestial bodies and the visible horizon. Referencing well-recorded positions of these bodies, an aircraft equipped with a celestial navigation system can accurately determine its current location, speed, and course. The main advantages of celestial navigation include its independence of ground aids, global coverage, immunity to jamming, and passive nature, but its accuracy is still far from that of GPS. Nonetheless, this navigation method is present in several spacecraft, intercontinental ballistic missiles, and aircrafts such as the SR-71 [64]. Like INS, celestial navigation is a historically reliable navigation system that can be coupled with GPS or other navigation systems to allow for a constant position and location validation in the case of GPS jamming or spoofing.

3. Radar/Infrared/Laser Navigation

Several different navigation systems rely on the transmission of electromagnetic (EM) waves. EM-based navigation systems include radar, infrared trackers, and optical sensors. While active and passive guidance systems based on the radar is present on missiles, light detection and ranging (lidar) is an excellent possible navigation system that is a widely used method to control and navigate autonomous systems. Lidar uses several lasers to measure its distance to a surface by measuring the reflection with a sensor. As a result, lidar can accurately map out terrains and determine a body's distance to a specified surface. Combined with recent improvements in range and tolerance to rain and dust, lidar is a vital part of a lightweight, comprehensive vision system that can support the primary navigation systems [6]. The drawbacks of lidar involve its current high cost and inability to work in zero visibility conditions. Regardless, lidar can provide periodic corrections and validations alongside GPS and INS and is another one of many different types of navigation systems that can accurately support a primary navigation system [65].

V. Proposed Solution

Taking into consideration the concepts of UAM proposed by the government and commercial agencies, this section provides a coherent infrastructure that ensures secure data links. Incorporating the aircraft systems outlined in Section (II) that are vulnerable to the attacks described in Section (III), a combination of anti-jamming technology, secondary systems, encryption, and blockchain would allow for secure operations of a scalable UAM environment. The proposed scheme is displayed below in figure 2.

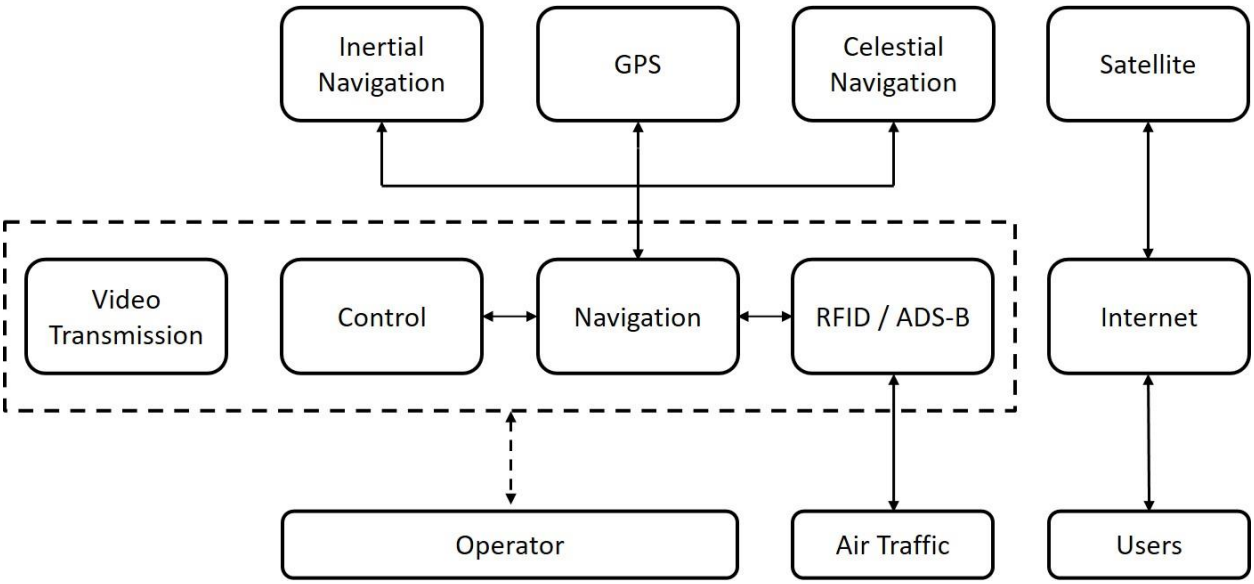

Figure 2. Proposed Telemetry and Data Links for Flying Cars

C. Autonomous Flight for Secure Controls, Navigation, Video Transmissions, and ADS-B

It is essential to consider all data links jammable when devising a safe communication system for controls, video transmissions, and navigation. Jamming is the only physical cyberattack, and thus there always will be a possibility of jamming, regardless of the number of direct anti-jamming techniques. As a result, it is important to imagine a flying car without any wireless connections. The resulting safest operations are fully autonomous operations. The realization that full autonomy is one of the very few solutions to jamming has led many agencies to expect the UAM environment to rely on primarily autonomous flight trips. The manual controls would then serve as a backup and safety measure [3, 6]. In this case, the primary control data link is between the on-board aircraft computers and a centralized management system to provide the trip's flight plan. This communication would ideally occur only when the aircraft is stationary and possibly through a physical wired connection. With the aircraft securely loaded with an autonomous flight plane, the aircraft is now dependent on the navigation system to execute the flight plan. The secondary control link is the traditional direct connection to a remote pilot that can control the aircraft in the case of an emergency in combination with the video transmissions and navigation information. The combination of video transmissions, secondary controls, and navigation information enables a feasible approach in creating a manageable PKI that allows for secure encryption. Manufacturers can establish a tertiary control data link through satellite communication for BLOS as safety precautions. However, this addition may be costly and unnecessary.

Given the absence of jamming and current technical limitations, all wireless data links can operate in LOS. The propulsive range of flying cars is currently between 50 – 100 miles, and a UAM environment can take place comfortably in this range using only standard antennas [6]. Employing only LOS operations would minimize latency associated with BLOS communications and allow a less costly and simpler means of securing the overall aircraft.

D. Navigation

With flying cars relying primarily on their navigation systems to execute a flight plan, the most important data link for a moving flying car is its navigation system. Although GPS is very precise and well developed, other navigation systems would support the GPS that still is the primary navigation system. Like the now wired primary data link, the most appropriate and secure navigation system is immune to jamming and spoofing. Inertial, celestial, and radar/infrared/laser navigation systems all offer excellent alternatives. In practice, two additional navigation systems, such as an INS and celestial navigation system is sufficient to validate a GPS signal. However, to ensure comparable accuracy to GPS, a third additional navigation system such as lidar or active radar may help flying aircraft pinpoint their location or landing. The primary disadvantage of secondary systems is the added cost and weight, thus further development and testing is needed to find an economic balance of safety and performance amongst the possible systems. The dependency on secondary systems will avoid the need for encrypted GPS signals.

In a hypothetical example, a flying car can take off and begin to execute its flight plan, but some time during its flight, a hacker jams and spoofs all wireless connections, even if the aircraft employs a form of SS. The aircraft understands that its connections are jammed or spoofed through statistical analysis of the incoming signals or validation with the calibrated inertial navigation and celestial navigation, thus causing it to begin to ignore its GPS connection. The aircraft then relies on its inertial and celestial navigation systems that operate with no external input to travel to its destination. Near the destination, lidar or radar systems can help the aircraft identify a landing vertiport with high accuracy. As the aircraft nears its destination, there is a higher chance that an antenna at the destination may help an operator overpower the jamming signal and establish an authentic connection, but this cannot be guaranteed.

E. Encryption and Blockchain

With the video transmission, a secondary control link, and navigation information condensed into a single data link, blockchain can quickly implement encryption. This encryption can apply to this combined link, RFID tags, and an ADS-B system. Serving multiple purposes, blockchain can establish the PKI to validate important encryption keys while also organizing and tracking UAMs. Following an air taxi service model, blockchain can track and record transactions and flight information associated with each flight. This information may include information on the riders, the remote pilot, financial records, and the aircraft's critical information, such as the remaining fuel/battery, location, and flight plan. Ultimately the only two data links that occur on two different frequencies are the combined data link, ADS-B connection with air traffic, and RFID reading with authorized parties. The blockchain can implement a symmetric encryption key system to secure the secondary data link, and it can implement an asymmetric encryption key system to secure the ADS-B connection and RFID tags. The separation of these encryption types ensures safe communications of the data links with minimal creation of keys that can access the sensitive information. The creation of a single symmetric key to access the secondary data link keeps the encryption latency at a minimum while also stressing the importance of these keys' physical security. With one key corresponding to each flying car, the governing body that manages the fly cars' operations can likely keep all keys in a secured operating center that only the remote pilots and authorized personnel may access. With an asymmetric encryption scheme for the ADS-B system, the FAA can distribute the public keys to new vehicles as they enter the airspace. The FAA, established secure air traffic controllers, and aircraft manufacturers can keep the private keys to decrypt and read the transmitted ADS-B signals and RFID tags. This one-way communication allows for easy integration of future flying cars and the assurance that only authorized parties are receiving the aircraft's information. A blockchain system used to distribute the keys will consistently authenticate each key and ensure no modifications to keys.

F. Internet

With the navigation, control, and video data stream from the flying car directly encrypted to a control center, the only presence of the internet would be if the vehicle manufacturers want an internet connection for passengers, similar to normal commercial aircraft. However, these connections are at the mercy of the satellite owners, and sometimes these connections remain unsecured. In addition, no federal or commercial agency will likely invest in developing an encrypted satellite connection. Thus, the only foreseeable condition for the internet on flying cars is with the help of existing satellite internet providers such as Gogo Inc, Panasonic, and Viasat. However, experts have long pointed out that these providers use little to no encryption or unsecured certificates [66]. Ultimately, flying cars should not rely on internet providers to add the layers of encryption necessary for secure in-flight internet connections. One possible secondary solution is virtual private networks (VPNs) to redirect traffic through an encrypted connection. However, this adds latency to the already high-latency connection. Unfortunately, there are no other economical solutions to providing a more secure in-flight internet connection, and passengers should continue to avoid accessing sensitive information while in flight.

VI. Conclusion

This research summarizes several cybersecurity vulnerabilities and cybersecurity incidents of UAVs and commercial aircraft relevant to UAM. With the exact operations of UAM still under development, it is vital to develop the policies and technologies that ensure secure airspace. As a result, UAM offers a unique opportunity to the cybersecurity world to create an intricate and secure system for a service that will revolutionize modern transportation. This paper analyzes threats, recent incidents, and current solutions while proposing a holistic infrastructure to support UAM. Resilient to jamming, spoofing, DOS attacks, MITM, and other cyber-attacks, the proposed system includes:

- Fully autonomous flight supported with physical loading of the flight map plans
- Multiple inter-validating navigation systems
- Symmetric encryption for combined video transmission, secondary control, and navigation data link
- Asymmetrically encrypted ADS-B and RFID tags for air traffic controllers and law enforcement
- Blockchain-based PKI for management of keys
- Exclusion of in-flight internet or usage with a VPN

With these appropriate measures, flying cars can operate securely in the national airspace and begin building public acceptance. Public acceptance will likely be one of the most difficult obstacles for UAM but establishing cybersecurity systems shows an initiative and desire from government and private companies to place users' safety first. While it may take several years, these policies will eventually allow other aircraft and UAVs to become integrated into the AAM initiative.

VII. Acknowledgments

This effort is funded by the NASA Aeronautics Research Mission Directorate. The author thanks Steve Garcia, Ken Freeman, Helen Euler, and Bimal Aponso of the Secure Airspace program for their support and constructive criticism of this study.

References

[1] F. A. Administration. "14 CFR § 107.1 - Applicability." Legal Information Institute. https://www.law.cornell.edu/cfr/text/14/107.1 (accessed July 8, 2020).

[2] F. A. Administration. "UAS Remote Identification." https://www.faa.gov/uas/research_development/remote_id/ (accessed August 7, 2020).

[3] S. Bradford. "Urban Air Mobility (UAM) Concept of Operations." Federal Aviation Administration. (accessed July 15, 2020).

[4] D. P. Thipphavong *et al.*, "Urban air mobility airspace integration concepts and considerations," in *2018 Aviation Technology, Integration, and Operations Conference*, 2018, p. 3676.

[5] A. P. Air, "Revising the airspace model for the safe integration of small unmanned aircraft systems," *Amazon Prime Air*, 2015.

[6] J. Holden and N. Goel, "Uber elevate: Fast-forwarding to a future of on-demand urban air transportation. Uber Technologies," *Inc., San Francisco, CA*, 2016.

[7] D. Mototolea, "A study on the actual and upcoming drone communication systems," in *2019 International Symposium on Signals, Circuits and Systems (ISSCS)*, 2019: IEEE, pp. 1-4.

[8] T. S. Farmakis and R. D. Routsong, "Satellite based aircraft traffic control system," ed: Google Patents, 1998.

[9] A. Roy, "Secure aircraft communications addressing and reporting system (ACARS)," ed: Google Patents, 2004.

[10] A. J.-M. Bothorel, "Radio communication system for ACARS messages exchange," ed: Google Patents, 2013.

[11] F. A. Administration. "Aircraft Situation Display to Industry (ASDI)." (accessed.

[12] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78-87, 2011.

[13] F. A. Administration, "14 CFR § 91.225 - Automatic Dependent Surveillance-Broadcast (ADS-B) Out equipment and use.," ed. https://www.law.cornell.edu/cfr/text/14/91.225: Legal Information Institute, 2010.

[14] D. L. McCallie, "Exploring Potential ADS-B Vulnerabilites in the FAA's Nextgen Air Transportation System," AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH DEPT OF ELECTRICAL AND …, 2011.

[15] "Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft," U. S. G. A. Office, Ed., ed. https://www.gao.gov/products/GAO-18-177: U.S Government Accountability Office, 2018.

[16] "Revision to Automatic Dependent Surveillance-Broadcast (ADS–B) Out Equipment and Use Requirements," ed. https://www.govinfo.gov/content/pkg/FR-2019-07-18/pdf/2019-15248.pdf: Federal Aviation Administration, 2019.

[17] Y. S. Chang *et al.*, "Development of RFID enabled aircraft maintenance system," in *2006 4th IEEE International Conference on Industrial Informatics*, 2006: IEEE, pp. 224-229.

[18] I. Bor-Yaliniz, M. Salem, G. Senerath, and H. Yanikomeroglu, "Is 5G ready for drones: A look into contemporary and prospective wireless networks from a standardization perspective," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 18-27, 2019.

[19] B. A. Lauer, J. Stamatopoulos, A. Rashid, J. A. Tobin, P. J. Walsh, and S. J. Arntzen, "System for creating an aircraft-based internet protocol subnet in an airborne wireless cellular network," ed: Google Patents, 2011.

[20] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68-74, 2018.

[21] C. Pu, "Jamming-resilient multipath routing protocol for flying ad hoc networks," *IEEE Access*, vol. 6, pp. 68472-68486, 2018.

[22] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75-81, 2018.

[23] K. Wesson and T. Humphreys, "Hacking drones," *Scientific American*, vol. 309, no. 5, pp. 54-59, 2013.

[24] Y. Lee, Y. Kang, S. Lee, H. Lee, and Y. Ryu, "An overview of unmanned aerial vehicle: Cyber security perspective," *Korea*, vol. 12, p. 13, 2012.

[25] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, 2017: IEEE, pp. 194-199.

[26] J. Keller, "Iran–US RQ-170 incident has defense industry saying ‘never again’to unmanned vehicle hacking," *Military & Aerospace Electronics, May*, vol. 3, 2016.
[27] S. Shane and D. E. Sanger, "Drone crash in Iran reveals secret US surveillance effort," *The New York Times*, vol. 7, 2011.
[28] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1-16, 2012.
[29] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal," *Journal of Positioning, Navigation, and Timing*, vol. 4, no. 2, pp. 57-65, 2015.
[30] S. P. Arteaga, L. A. M. Hernández, G. S. Pérez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo," *IEEE Access*, vol. 7, pp. 51782-51789, 2019.
[31] N. Rodday, "Hacking a professional drone," *Slides at www. blackhat. com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone. pdf*, 2016.
[32] S. Kamkar, "SkyJack," *Github. com*, 2013.
[33] J. Crook, "Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones," *TechCrunch*, 2013.
[34] L. Kellon, "Parrot drones ‘vulnerable to flying hack attack’," ed: Dec, 2013.
[35] J. Tewes, "Cybersecurity as Airworthiness," *Available at SSRN 3033898*, 2017.
[36] A. Koubâa, B. Qureshi, M.-F. Sriti, Y. Javed, and E. Tovar, "A service-oriented Cloud-based management system for the Internet-of-Drones," in *2017 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, 2017: IEEE, pp. 329-335.
[37] A. Koubâa *et al.*, "Dronemap planner: A service-oriented cloud-based management system for the internet-of-drones," *Ad Hoc Networks*, vol. 86, pp. 46-62, 2019.
[38] R. Chaâri *et al.*, "Cyber-physical systems clouds: A survey," *Computer Networks*, vol. 108, pp. 260-278, 2016.
[39] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile Internet of Things: Can UAVs provide an energy-efficient mobile architecture?," in *2016 IEEE global communications conference (GLOBECOM)*, 2016: IEEE, pp. 1-6.
[40] I. Flechais, G. Chalhoub, N. Nthala, R. Abu-Salma, and E. Tom, "Factoring user experience into the security and privacy design of smart home devices: A case study."
[41] M. Guri, B. Zadov, and Y. Elovici, "LED-it-GO: Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED," in *International conference on detection of intrusions and malware, and vulnerability assessment*, 2017: Springer, pp. 161-184.
[42] M. Lehto, "Cyber Security in Aviation, Maritime and Automotive," in *Computation and Big Data for Transport*: Springer, 2020, pp. 19-32.
[43] M. Hooper *et al.*, "Securing commercial wifi-based uavs from common security attacks," in *MILCOM 2016-2016 IEEE Military Communications Conference*, 2016: IEEE, pp. 1213-1218.
[44] R. Santamarta, "A wake-up call for SATCOM security," *Technical White Paper*, 2014.
[45] S. F. Bichler, "Mitigating cyber security risk in satellite ground systems," Air Command And Staff College Maxwell Air Force Base United States, 2015.
[46] R. Santamarta, *Last call for SATCOM security*. IOActive, 2018.
[47] A. Costin and A. Francillon, "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," *Black Hat USA*, pp. 1-12, 2012.
[48] B. Haines and N. Fostrer, "Spoofing ADS-B," *from" Hackers+ Airplanes= No good can come of this" presented at Defcon*, vol. 20.
[49] M. Strohmeier, V. Lenders, and I. Martinovic, "Lightweight location verification in air traffic surveillance networks," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 2015, pp. 49-60.
[50] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," *IEEE internet of things journal*, vol. 6, no. 2, pp. 2103-2115, 2019, doi: 10.1109/jiot.2018.2869847.
[51] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005, pp. 46-57.
[52] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *IEEE Transactions on dependable and secure computing*, vol. 9, no. 1, pp. 101-114, 2011.
[53] E. Biham and A. Shamir, *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.
[54] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption," *International Journal of Computer Science and Engineering*, vol. 1, no. 1, pp. 70-75, 2007.

[55] P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," *Global Journal of Computer Science and Technology*, 2013.
[56] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Annual International Cryptology Conference*, 1999: Springer, pp. 537-554.
[57] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1994: Springer, pp. 92-111.
[58] T. Hardjono and L. R. Dondeti, *Security in Wireless LANS and MANS (Artech House Computer Security)*. Artech House, Inc., 2005.
[59] T. K. Meehan, J. B. Thomas Jr, and L. E. Young, "P-code enhanced method for processing encrypted GPS signals without knowledge of the encryption code," ed: Google Patents, 2000.
[60] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.
[61] M. Pilkington, "Blockchain technology: principles and applications," in *Research handbook on digital transformations*: Edward Elgar Publishing, 2016.
[62] R. Reisman, "Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy," in *AIAA Scitech 2019 Forum*, 2019, p. 2203.
[63] S. Nassar, *Improving the inertial navigation system (INS) error model for INS and INS/DGPS applications*. University of Calgary, Department of Geomatics Engineering, 2003.
[64] M. Belenkii, D. Bruns, T. Brinkley, and G. Kaplan, "Angles only navigation system," ed: Google Patents, 2009.
[65] Y. Gao, S. Liu, M. M. Atia, and A. Noureldin, "INS/GPS/LiDAR integrated navigation system for urban and indoor environments using hybrid scan matching algorithm," *Sensors*, vol. 15, no. 9, pp. 23286-23302, 2015.
[66] A. R. Taleqani, K. E. Nygard, R. Bridgelall, and J. Hough, "Machine Learning Approach to Cyber Security in Aviation," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 2018: IEEE, pp. 0147-0152.