Simulation and Modeling Concepts for Secure Airspace Operations

Banavar Sridhar*, Gano Chatterji† and Kenneth Freeman‡
NASA Ames Research Center, Moffett Field, CA, 94035-1000

This paper examines cyber security vulnerabilities of Urban Air Mobility operations. With the expected advent of new entrants including Unmanned Aerial Systems, Commercial Launch Vehicles and Urban Air Mobility aircraft, the future United States National Airspace System will have to evolve to include their operations along with the current commercial, general aviation and military operations. The National Aeronautics and Space Administration and the Federal Aviation Administration are working together to provide a vision for aviation operations in the future—2045 and beyond. Their National Airspace System Horizons initiative seeks to provide stakeholders a list of operational scenarios and technologies, concepts and strategies needed for supporting that vision. They have identified cybersecurity as one of the seven strategic interest areas for realizing this vision. Consequently, NASA is studying cyber resiliency for secure airspace operations. While there are many pathways to attack a cyber physical system such as Urban Air Mobility, their effect is expressed in modification or corruption of data/information used for controlling vehicles and making operational decisions. The paper describes cybersecurity technologies of Encryption, Blockchain, Virtual Information Fabric Infrastructure, Trusted Platform Module and Anomaly Detection for protecting the data, and the cyber resiliency of the current and future air traffic management system.

I. Introduction

The developments in Urban Air Mobility (UAM) — on demand flights with two to six passenger aircraft — and Unmanned Aerial System (UAS) — package delivery drones — will introduce a large amount of low altitude air traffic into the National Airspace System (NAS). These classes of low-cost vehicles will need to be integrated with the current NAS supporting air transportation in the United States. National Aeronautics and Space Administration (NASA) and the Federal Aviation Administration (FAA) have been developing concept-of-operations for the safe and efficient integration of the operations of these new classes of vehicles in the NAS. NAS Horizons[1] is an initiative by NASA and the FAA to provide a vision for aviation operations for the future — 2045 and beyond. The objective of this initiative is to develop a list of airspace scenarios and technologies, concepts and strategies needed for supporting the 2045 and beyond vision.

The FAA concept of operations for UAM is designed to support the growth of low flying and electric Vertical Takeoff and Landing (eVTOL) aircraft operating between vertiports — aerodromes — for transporting people and cargo in urban areas, inter-city and in underserved regions. The concept divides airspace into three regions: (a) ATM, all airspace currently used by conventional air traffic, (b) UAM, a corridor between vertiports for operation of UAM and suitable equipped aircraft and (c) UTM, UAS operating at or below 400 feet above ground level. Aircraft inside the UAM corridor will be governed by specific rules including community-based rules, procedures and performance requirements. The rules allow for UAM aircraft and other aircraft to cross the corridor. Operations within the corridor are expected to be conducted without support from FAA separation services in normal conditions. Operations outside the corridor are subject to Air Traffic Management (ATM) rules, including for onboard equipment and communication with Air Traffic Control (ATC).

The concept-of-operation expects UAM traffic operations to evolve gradually from flying on current helicopter route infrastructure to flying mostly within the corridors. This transformation will be characterized by high levels of automation, especially needed for ensuring safe separation between UAM aircraft. UAM is expected to be a community-based, collaborative traffic management system with operators coordinating, managing and executing operations within the FAA established legal framework. The architecture developed under the NASA Unmanned

* Principal Scientist, USRA at NASA Ames Research Center, MS 210-8, Fellow.
† Senior Scientist and Lead, Crown Consulting, Inc., MS 210-8, Associate Fellow.
‡ Aerospace Engineer, NASA Ames Research Center.

Aircraft System Traffic Management (UTM) project with various air traffic services provided by one or more organizations is considered a model for developing UAM air traffic services. UAM, like the envisioned UTM system, will provide federated services for enabling collaborative management of operations between flight operators, supported by their service suppliers — Providers of Services to UAM (PSU) — exchanging information digitally using data-communication networks.

The geographically distributed UAM network will enable exchange of data and information between UAM operators, PSUs, FAA and public interest stakeholders such as law enforcement, cities and safety organizations. Figure 1 shows an example of logical communication links between stakeholders including service providers. The physical network will consist of sensor, communication, compute and storage nodes. Data will be transported over wired data-communication networks and wirelessly — using airband radio and satellite communication — between the UAM-aircraft, between satellites and ground stations and between UAM-aircraft and ground-based systems. This cyber-

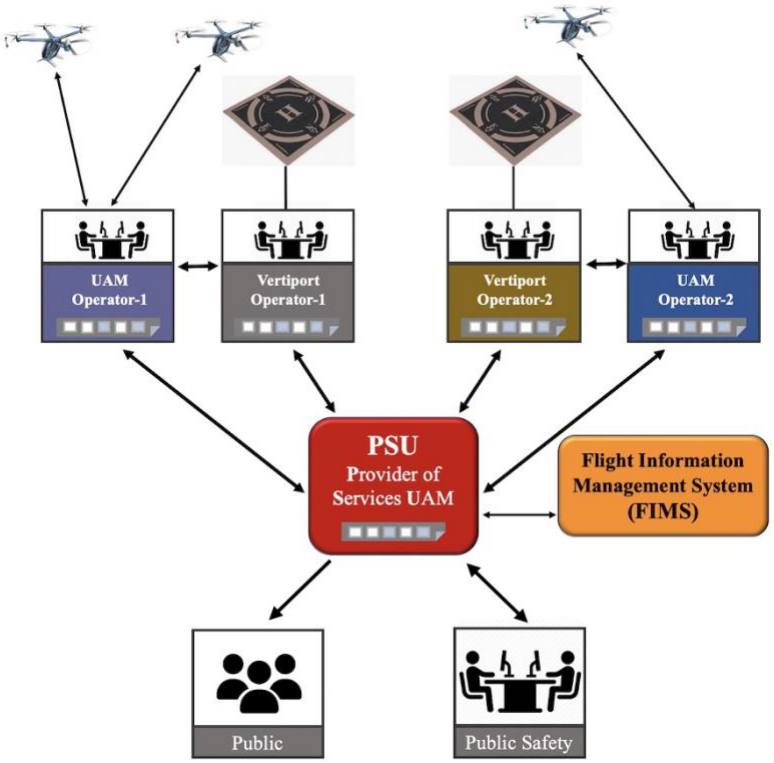

Figure 1. Interaction between UAM system participants.

physical world of interconnected and interdependent systems increases the vulnerability of aircraft and air traffic management systems to cyberattacks especially with resourceful state actors. The impact of security breaches includes potential of both economic harm and loss of life. Cybersecurity has been identified as one of the seven strategic interest area in the NAS Horizons report.[1]

To determine that the system is operating safely and efficiently given the operational conditions, and to make decisions for ensuring safe and efficient operations in the presence of uncertainties, failures and malicious attacks, a data and reasoning fabric is required. Data is essential because it contains information about the state of the system — and its components — the outcome of previous decisions and the dynamics of the system. Metrics derived from these data can be used to ascertain the performance of the system. Data fabric is defined as the environment for enabling sharing and access of data in a distributed data environment. The data fabric consists of technologies, policies and processes implemented in a consistent data management architecture for enabling organizations to maximize the value of their data. Reasoning is required for determining the correctness of data, state of the system and for making decisions. Reasoning can be implemented with a deep understanding of the system using rules, logic and analysis techniques based on optimization, machine learning and decision sciences.

Given the central role of data in making decisions that affect both the safety and efficiency of operations, the paper explores cybersecurity technologies of Encryption, Blockchain, Virtual Information Fabric Infrastructure, Trusted

Platform Module and Anomaly Detection for protecting the data. Protecting the data from unauthorized modification will improve the cyber resiliency of the current and future air traffic management system. The rest of the paper is organized as follows. Wireless technologies and security issues of communications in mobile networks is discussed in Section II. Approaches for establishing the reliability of data (source, accuracy, completeness and consistency of data) are briefly outlined in Section III. Cyber security technologies are discussed at length in Section IV. NASA's UAM maturity levels are briefly described and the importance of cybersecurity in achieving the goals are emphasized in Section V. The paper is concluded in Section VI.

II. Security Issues in Mobile Networks

Wireless Communication (WC) is anticipated to be ubiquitous in the UAM system. The Communication, Navigation, Surveillance and Information (CNSI)) networks use Automatic Dependent Surveillance-Broadcast (ADS-B), Global Positioning System (GPS) and 4G and 5G infrastructure.[2-3] ADS-B-equipped aircraft and vehicles exchange information on one of two frequencies: 978 MHz or 1090 MHz. Mode A/C and S transponders, as well as Traffic Collision and Avoidance Systems (TCAS), use 1090 MHz. GPS uses two frequencies L1 at 1575.42 MHz and L2 at 1227.6 MHZ.

The G in wireless stands for generation. Initially analog, wireless became digital in 2G. The current 4G systems support 100 Mbps at a latency of less than 100 ms since 2011. 5G networks that promise 20 Gbps with a latency of less than 5 ms are being deployed currently on existing 4G infrastructure by improving bandwidth, capacity and reliability. The 1G to 4G networks operate in the frequency range 850 MHz to 2.5 GHz. The use of low band radio frequencies in 1-4G networks enables transmission of data through walls and other material and over long distances. It can use large cell towers to cover geographical areas. Use of high frequency in 5G such as millimeter wave will increase speed at the cost of reduced penetration through barriers and shorter transmission range.

The low (< 2.5 GHz), medium (2.5 to 10 GHz) and high (10 to 100 GHz) frequencies of the 5G spectrum used for transmitting and receiving signals offer different advantages and present their own challenges[2]. 5G uses three different types of technologies: Enhanced Mobile Broadband (EMBB), Ultra-Reliable Low-Latency Communications (URLLC) and Massive Machine Type Communications (MMTC). EMBB supports HDTV and prioritizes speed. URLLC supports mission critical activities with a latency of less than 5 ms and uptime availability of 99.999%; it is suitable for UAM applications such as for vehicle-to-vehicle (V2V) communications. MMTC supports fast download speed; it prioritizes connectivity to many devices. Service providers use a combination of radio frequencies to achieve the speed, range and other objectives of EMBB, URLLC and MMTC.

The demand for 5G in aviation is driven by the need for data exchange between aircraft for separation assurance, and between aircraft and ground station for guidance, navigation and control of the aircraft; health-monitoring and prognostics; relay of air traffic and operator voice and digital communication; and real time transfer of mission data. Information exchange for supporting increased automation of the UAM system, communication between PSUs and UAM aircraft, and safety and security critical functions might require the high data transfer rate with stringent latency requirements provided by 5G technologies, which in addition to supporting voice communication, offer 100 times faster data rate than 4G to the end users.

The present ATM system is closed in that it is regulated and operated by the single air traffic service provider, which in the US is the FAA. The current system would need to expand significantly to accommodate the large increase in air traffic caused by the operations of new entrants such as package delivery drones and UAM aircraft. This is highly unlikely because scaling up the current system with the humans and equipment needed would burden the government with significant sustained financial commitment. The proposal therefore is for developing industry financed community-based systems in which the stakeholders collaborate and exchange information with each other, and exchange information with the ATM system for achieving safe operations. To rapidly build these systems and reduce cost, the industry will use Commercial Off-The-Shelf (COTS) and open-source hardware and software products. While this approach offers significant benefits in terms of cost and time to market, it has the potential of introducing components into the system that were not designed for cyber resilience, thereby, increasing the vulnerability of the system to external attacks and failure.

Data broadcast using the wireless spectrum for communication between parties results in many security issues that are not yet well-understood, and need to be modeled. An aircraft traveling between two locations transmits and receives significant amounts of information critical for maintaining safety of passengers and crew. Aircraft connect to the internet via satellite or via terrestrial mobile services (3G,4G network). There are significant limitations in speed and latency. Cellular networks provide near complete coverage in urban areas. Cellular networks can handle orders of more data than aviation networks. However, 4G networks are not designed to handle critical applications. They have

long-distance line-of-sight problems. They need risk mitigation during interruption of service. Traditional security systems employ static, legacy-type and fixed policy-based approaches controlled from within an enterprise system for protecting data and network access to it. Aircraft dependent on Mobile Communication Devices (MCD) with data storage and software applications connected to enterprise networks create new challenges because an actor with malicious intent can configure hardware, software and operating systems without authorization from a trusted authority. Secure Airspace Operations (SAO) therefore need security systems with static and dynamic security elements for ensuring compliance with security policies, including those for mitigating MCD vulnerabilities.

The security of a cyber physical system includes protecting both the information and the means for accessing it (network). Networks are often subjected to passive and active attacks. The objective of passive attacks is to secure a foothold and stay dormant till activated to attack the system. Active attacks seek to compromise integrity, authenticity and confidentiality of the data, control access and overwhelm the system resources (denial-of-service attack). Network security should therefore be an integral part of the design and operation of the system and not an afterthought.

The National Institute of Standards and Technology (NIST) cybersecurity framework[4] provides industry standards, guidelines and practices to conduct cybersecurity operations at various levels. The Framework Core is a set of five concurrent and continuous functions: Identify, Protect, Detect, Respond and Recover. Identify develops an understanding of management of cybersecurity risks to systems, people, assets, data and capabilities. Protect develops and implements the necessary safeguards against threat vectors. Protect functions include identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance and protective technology. Detect develops and implements means for timely discovery of threat events. Examples of the Detect function are anomaly detection and continuous monitoring of data transport across network interfaces. Respond develops and implements mitigating actions in response to detected cybersecurity events/incidents for example quarantining malicious code. Recover develops and maintains cyber resilience plans and implements them to restore services and the normal functioning of the system impaired by a cybersecurity event. The Recover function consists of recovery planning, procedures and communications for enabling timely recovery to normal operations.

Networks are often secured by implementing security services that utilize cryptographic techniques. Cryptography enables two sources to exchange sensitive information in a secure way using algorithms based on the use of prime numbers and modulo arithmetic. Confidentiality prevents disclosure of protected user information without permission. Authentication assures the source of information and the user seeking it are both legitimate (have the required credentials). Dependability is an integrated concept consisting of availability, reliability, safety, security and resilience. Availability is the ability of the system to provide the services as needed. It includes the readiness and the continuity of the needed service. Reliability is the ability of the system to deliver the services as specified. Safety is the ability of the system to operate without catastrophic failure affecting neither the user, nor the environment. Security is the ability of the system to protect itself against deliberate — malicious — and unintended — accidental — intrusion. Security also adds confidentiality to dependability. Finally, resilience is the ability of the system to mitigate and recover from harmful events.

Redundancy is frequently employed to enhance fault tolerance. Redundancy is achieved by duplication of the hardware and software for accomplishing the same task. For example, the location of the aircraft can be determined independently by two GPS systems. Non-repudiation is an attribute where the originator of the information cannot deny originating the information; for example, the signatory on a notarized contract cannot deny signing the contract.

III. Data Reliability in Secure Airspace Operations (SAO)

Data reliability refers to the accuracy and completeness of computer-processed data. The authenticity of the source of the data and its correctness for the function being performed needs to be established based on objective metrics for ensuring data reliability. There are several different techniques that can be applied to establish data reliability. For example, a database of normal events can be created by logging actual events and labeling them as such based on inspection and then comparing real-time events against the labeled data in the database to ascertain whether the real-time data are normal or not. One could also use simulated data with known parameter bounds to create such a database for comparison against real-time event data. The correctness of the data can be established by checking for units such as nautical miles for distances and seconds for time, data bounds such as within plus-minus two minutes, relation between data elements such as distance is the product of speed and time, time derivative of speed is acceleration, and difference in the data provided by redundant sensors and processes.

Research in SAO needs to address: (a) architecture for information exchange best suited for secure interaction between multiple agents and stakeholders of airspace operations, (b) authentication and authorization of the sources and system components for accessing services and establishing trust and (c) methods for validating data integrity — accuracy, completeness and consistency of data. These types of cybersecurity requirements are common to

complex problems involving many decision-makers, e.g., automation of ground transportation. SAO needs to adapt the evolving cybersecurity technologies described in the next section with an architecture which supports increasing levels of maturity.

Authentication of the source can be established during runtime by checking the encrypted token (certificate) provided by the source with the authentication and authorization (A&A) agent that either accepts the certificate provide by the source directly if the A&A is also the certificate issuing authority or sends it to a certification issuing authority to establish authentication of the source. Once the authentication is established, the A&A agent returns the authorization information to the calling service for the service to grant access to the source as authorized.

IV. Cybersecurity Technologies

Encryption

Encryption facilitates confidentiality for exchange of data between two parties by converting plaintext information to unintelligible ciphertext using algorithms. There are two types of encryption techniques: symmetric encryption (SE) and asymmetric encryption (AE). SE uses the same secret key to both encipher and decipher messages. It is fast, easy to implement in hardware and widely used in practice. SE works well for a small group of authorized users but does not scale well for large groups. The key must be exchanged via a trusted channel. Some of the disadvantages of SE are the fixed length, susceptibility to being stolen and difficulty of key management administration. Some examples of SE systems are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (TDEA), which is also known as 3DES, and International Data Encryption Algorithm (IDEA).

The AE method employs the Public Key Infrastructure (PKI) to achieve data confidentiality by using a pair of keys — a public key and a private key. The public key is available to everyone and the private key is available only to authorized receivers. The PKI sends encrypted data to each receiver and requires processing overhead and bandwidth. Figure 2 shows the encryption of the message by the sender and decryption of the message by the receiver using the public and private keys. AE works well for a small group of authorized senders and receivers with pre-distributed keys. AE provides variable size keys and can be used for both encryption and digital signature. However, AE is relatively slow, inefficient for encrypting large amounts of data and has problems with authentication of public keys.

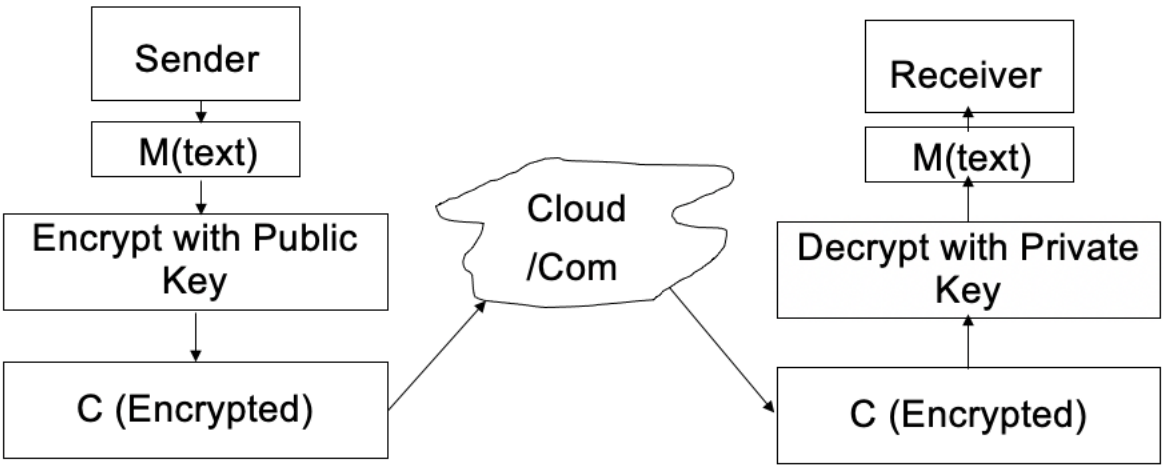

Figure 2. Flow of encrypted message

The most commonly used cryptography algorithms are RSA[5], Diffie-Hellman Key Exchange[6] and Elliptic Curve cryptography[7]. The algorithm consists of three steps, namely: key generation, encryption and decryption. The algorithms use prime numbers, random number generators and modulo arithmetic. The generation of keys should be random, independent and no part of the key should have any deterministic nature.

Hash functions are used extensively in cryptography algorithms to maintain data integrity. A Hash function is a one-way mapping from an arbitrarily long input message to a short finite length message. The hash function, h= H(M), where M is a variable length block of data and h is a fixed size hash value. A compression function, z = f(x, y), with inputs x, an input bit from a previous step (known as chaining variable) and y, a bit block, outputs a bit z. An initial

value is specified as part of the algorithm at the start of hashing. The Secure Hash Algorithm (SHA) iteratively uses the compress function. The SHA-512 is a member of the family of cryptographic hash functions with a message digest size 512, message size less than 2^{128}, block size 1024, word size 64 and 80 number of steps. The number of possible inputs to the hash functions can be infinite and the output size is finite. It is possible, but unlikely, that two different inputs produce the same hash output. SHA-512 is said to be collision resistant because to find a collision in SHA-512, an algorithm must be executed approximately 2^{256} times. With the use of algorithms like SHA-512, security risks come from sources other than brute force attacks.

The Message Authentication Code (MAC), also known as keyed hash function or cryptographic checksum is a fixed length hash value and is defined by the function, MAC=C(K,M), where K is the secret key and M is a fixed length hash value.

Table 1 provides a list of some of the services used in cybersecurity and their components.

Table 1: Cybersecurity services and their components.

Service	Mechanism	Components
Confidentiality	Encryption	Symmetric or Asymmetric
Authentication Integrity Non-repudiation	Digital Signature	Asymmetric Private key encryption Hash function
Key Establishment	Key Agreement	Asymmetric Private key encryption
Authentication Integrity	Message Authentication Code	Key used to with hash function

Data Encryption Standard[8] (DES) for hardware implemented encryption algorithms were developed for the first time in 1976 and continue to be developed by NIST[4] and several other organizations. DES provides the user information about the level of security that can be expected from a secure system.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

A large-scale application such as Urban Air Mobility with distributed services and the need for supporting one-to-many communications requires efficient encryption mechanisms. Attribute-Based Encryption (ABE)[9] is a mechanism for efficiently implementing fine-grained access control in Internet-of-Things (IoT) applications. Each user has a list of attributes based on their role in the system. The basic ABE algorithm has four steps:

a) *Setup* — consists of randomized algorithm performed by a trusted authority to create the ABE scheme using an implicit security parameter without any inputs and outputs, a set of public parameters (PK) and a master key (MK)
b) *In Key Generation* — the trusted authority executes Setup to generate a secret key using attributes ω, PK and MK as inputs, and outputs a Decryption Key (SK)
c) *Encryption* — generation of the message m with a set of attributes ω' and public parameters PK is performed by the sender using a randomized algorithm resulting in the ciphertext output E
d) *Decryption* — takes as input encrypted ciphertext E with attributes ω', decryption key SK associated with ω and the public parameters PK. It outputs a message M if $|\omega \cap \omega'| >= d$, where d is a threshold parameter.

The dynamic nature of IoT requires ABE to be combined with an efficient attribute management system. Because attribute could be shared by many users at the same time, CP-ABE provides an efficient (without latency) revocation scheme without requiring encryption after every access policy change. The basic idea in CP-ABE is to split time into slots of variable durations. The time slots are determined according to user validity periods. Instead of renaming attributes for each time slot, a new one-way hash function returns a different result for each time slot. More details about the algorithm are provided in Ref.5.

Blockchain Technology

Blockchain technologies[10-11] can be used for identity management of vehicles, people and systems. It could be helpful for tracking transactions and verifying negotiated agreements between stakeholders in the NAS environment. For example, the record of the submitted flight plan and the approved flight plan could be verified using the Blockchain-based immutable ledger. Similarly, system and approval logs can be kept in an immutable ledger for audit

and accident and incident investigations. The use of blockchain technology for air traffic management was first proposed in reference 12.

A blockchain (BC) is a distributed system with either a linear structure or a graph-like structure with nodes and links connected without any centralized authoritative nodes or hierarchy. A user or an individual system is represented as a node within the blockchain network. A full node stores the entire BC made up of blocks. A publishing node is a full node which has the capability to extend the blockchain by creating and publishing new blocks. A lightweight node does not store or maintain a copy of BC and must pass their transactions to a full node.

Each block in the BC has a header containing metadata about the block, block data containing a set of transactions and other related data. Every block header (except the first one in the chain) contains cryptographic link to the header of the previous block. Each transaction involves one or more blockchain users, a recording of the changes and is digitally signed by the user submitting the transaction. The transaction is verified by all the nodes with their BC consisting of a copy of the chained blocks of all transactions.

Figure 3 shows a sequential timestamped blockchain and transfer of information from one block to the next block in the chain. Nonce is a random number that is used only once as a seed. A Merkle tree is a hierarchical data structure where the data are hashed and combined until there is a single root hash, Merkle Root Hash, that represents the entire structure.

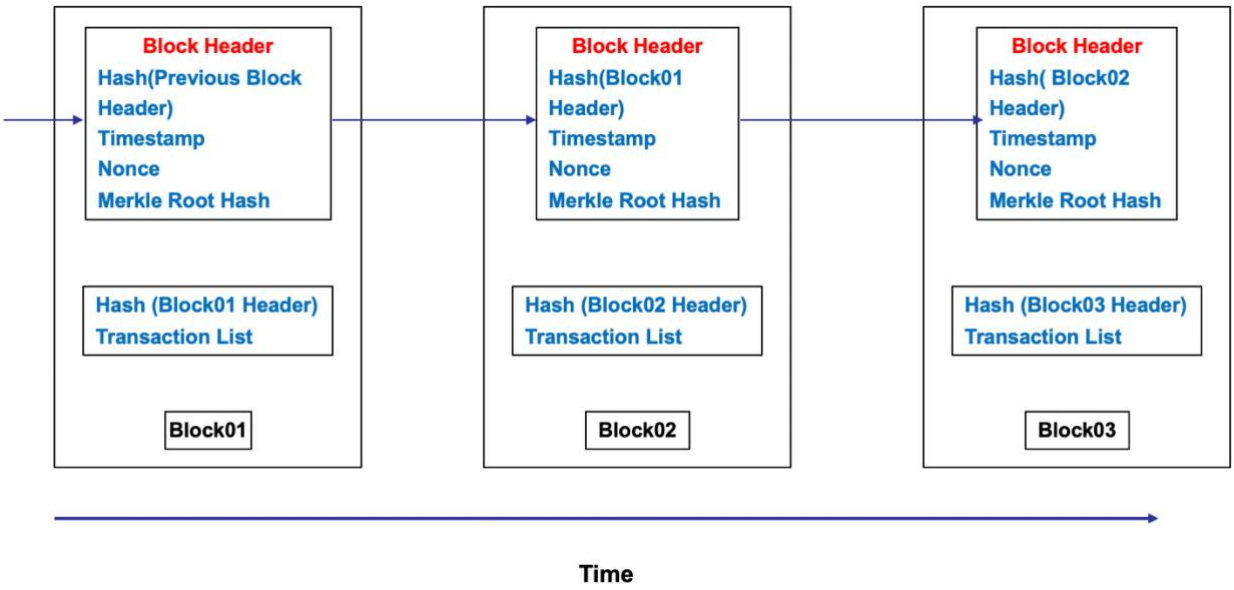

Figure 3. Sequential timestamped blockchain and block to block transfer of information.

There are two high level versions of blockchain. Permissioned blockchains limit users to recognized parties while permission-less blockchains are open to all. Users in a public BC can download the code into their own systems, modify it and use it according to their own requirements. The users in a public BC remain unidentified. Public BCs are widely used due to their openness and decentralization. They use complex protocols for security and consensus mechanism. Although public BCs provide privacy, they are prone to malicious attacks. They are also slow due to the amount of computation needed to achieve consensus; a typical transaction might need several minutes for approval.

A private BC is a permissioned system managed by an organization with pre-approved permission given to known participants for read and write operations. The known identities of validators (people who can approve transactions) and participants results in fewer complex mathematical operations to validate transactions on the network. The consensus algorithms use less energy and are fast with approval times of less than a second.

Consortium or federated blockchains are operated by a group of organizations with mutual interest. It is a permissioned system where all users can perform read operations. The write operations are limited to a few trusted users. Federated blockchains also use less energy due to voting based or multiparty approval-based consensus protocols. The transaction approval times are comparable to private BCs.

One of the central concepts of blockchain is forming consensus, which is the process for getting to an agreement between parties on whether a transaction is valid and if changes are permitted. Changes or additions to the BC can be made only if all nodes in the chain agree. For public BCs, the consensus mechanism works even when malicious nodes

are present. The proof-of-work is required in permission-less networks for a publishing node to publish the next block. Proof-of-work consists of expending time, energy and computational cycles to solve a hard-to-solve, but easy-to-verify problem. The publishing node sends the block with a valid nonce to full nodes in the blockchain network. The full nodes can easily verify the solution using the nonce, add the block to their copy of the blockchain and distribute it to their peer nodes. The publishing nodes are rewarded for their work after validation. Some public blockchain systems such as Bitcoin and Ethereum validate transactions after participation of at least 51% nodes on the underlying network using proof-of-work consensus protocol.[13,14] The level of difficulty of solving the problem is updated by controlling the number of leading zeros. Decreasing the number of zeros, increases the solution space, makes it easier to solve the problem. Conversely, increasing the number of leading zeros, reduces the solution space, which makes it more difficult to solve the problem. The adjustment to the level of difficulty is done to prevent a single user from taking control of the network and forcing others to perform extensive computations requiring significant amount of electricity consumption.

There are several other methods to reach consensus. Proof-of-Stake[15] method is one of them. It allows selected stakeholders in the network to create new blocks. Several different rules such as random validators and delegated validators are used in the selection of the validators. Proof-of-stake consumes less energy than the proof-of-work method. Byzantine fault tolerance[12] uses majority voting to prevent validation from malicious ones.

The different BC functions are implemented in the following layers: (a) a data layer consisting of data blocks, relevant encrypted messages and timestamp, (b) network layer, (c) consensus layer, (d) incentive layer with rewards mechanism, (e) contracts layer consisting of various types of script codes, algorithms, and sophisticated smart contracts and (f) an application layer supporting enterprise level applications and decentralized applications.

The blockchain technology is changing rapidly with the availability of new hardware and software platforms. With the emergence and adoption of cloud computing platforms, several organizations like Microsoft, Amazon, Google and IBM are providing blockchain-as-a-service to their customers.[16] There are many challenges in the application of BC technology such as privacy, scalability and side chains, blockchain security and smart contract vulnerabilities.[17,18] The speed of transactions in popular BC platforms is increasing rapidly;[19] it might now be possible to apply blockchain technology for establishing trust between interacting systems that is needed for SAO. Standards, interoperability requirements and regulations will have to be developed to successfully apply blockchain in aviation.

Virtual Information Fabric Infrastructure (VIFI)

The future networked UAM system will generate large amounts of data that will be stored in locations distributed throughout the network. Automation, decision-making, health and safety monitoring and predictive failure analytics will involve processing large volume of data using computational techniques such as estimation, physics-based predictions and machine learning. In the traditional approach, data from different locations are transported to the applications to perform the needed computations. The VIFI[20] concept proposes moving the applications to the data instead. It uses Docker containerization technology with the open-source workflow tool: Apache NIFI to achieve automated orchestration of distributed analytics, freeing users from possessing detailed knowledge of the distributed repositories and their underlying infrastructure. VIFI supports authorization control for data, metadata access, execution of models for clients without revealing private data, and the ability to integrate existing data owners using their policy for access. VIFI can be modified and customized for user applications.

Trusted Platform Module

Security in systems is usually achieved using secret keys and encrypted messages as described in the preceding paragraphs. Trusted Platform Module[21] (TPM) provides a hardware solution to this problem. A TPM chip is a secure processor that performs cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper resistant. TPMs are mainly used for secure boot, remote attestation and secure communication between computer systems in networks. The added security provided by TPM, like any other security method, can compete for computational resources that can delay safety critical functions, and the availability of the overall system. TPM functions can also be implemented in software. The major drawbacks of this type of TPM are the risk of internal bugs and attack from internal or external malicious software. Software-based TPM cryptographic algorithms also place additional computation load on the computer it is designed to protect.

The components of a TPM are (a) secure storage keys in volatile and non-volatile memory, (b) a Platform Configuration Register (PCR) for storing the current software and hardware state of the system, (c) encryption/decryption processors and (d) a random number generator. The PCR of the system changes with the state of the system and is computed by the equation

$$PCR_i^{t+1} = Hash(PCR_i^t || x(t))$$

where the PCR at the next time (t+1) depends on the hash digest of the previous PCR and the state of the system x(t). The PCR values build a chain of trust.

Anomaly Detection

Anomaly Detection is a method for identifying previously unseen behavior of a system. This implies that there is a notion of confidence bounds within which the system performs. Behavior outside of these established bounds (outliers) is indicative of abnormal or anomalous behavior. For example, Conformance Monitoring is often used in Air Traffic Management to verify that aircraft are following their planned route of flight or deviating from it. There are different types of anomalies. Point anomaly refers to situations where the position of the aircraft reported by a sensor compared to the earlier position report is not possible because of the aircraft's performance limits. Contextual anomaly refers to behavior of a system based on its operational mode. For example, the measured speed of an aircraft is incompatible with its current mode of flight (context) such as climb, descent or cruise. Some of the traditional techniques that have been used to detect anomalies are as follows. Exceedance analysis is based on knowing the behavior of the variables of the system (signatures) and checking if they stay within bounds. An example of exceedance analysis is verification that the initial climb speed of the aircraft is greater than the minimum climb speed specified by the aircraft manufacturer. Statistical analysis of the variables using metrics: mean, standard deviation and moments of the distribution is also used for anomaly detection. These traditional approaches are easy to implement, and useful for detecting known attack vectors, faults and failures. However, a challenge for SAO is that such approaches might not be able to detect emerging behavior (previously unknown) or new threats.

The availability of archived and real-time data can enable detection of emerging anomalous behavior using algorithms from data science and machine learning. The general approach is to build a profile/dataset of "normal behavior" and use the normal behavior characteristics to detect anomalous behavior, with the understanding that such behavior could be emergent and infrequent, and therefore difficult. The steps in anomaly detection are shown in Figure 4.

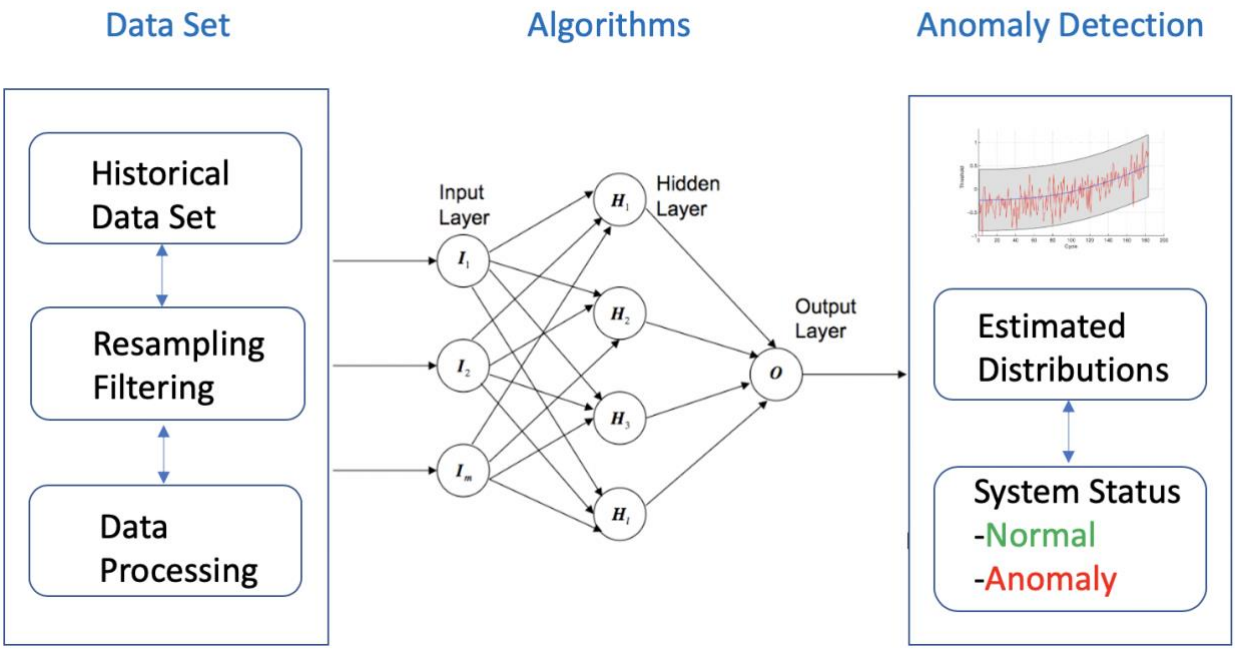

Fig 4. Steps in anomaly detection.

Algorithms[22] used for anomaly detection include Proximity-based methods, Density-based methods, Clustering-based methods, Support Vector Methods and Neural Networks. K-means is a popular unsupervised clustering algorithm which partitions data into K (usually specified by the user) number of groups. A special case is K=2 when data are divided into normal and anomalous groups. K-means clustering partitions the space into convex regions and the perpendicular line/hyperplane joining the centroids partitions the space between clusters. The algorithm: Mini-Batch K-means can be used to speed up computation when using large databases. Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is a data clustering algorithm that groups points using a local criterion such as

the density of points in a region, and region-growing to reduce the number of groups. Spectral clustering[23] is a graph-theoretical grouping method that uses eigenvectors derived from distance matrices and from affinity matrices to cluster. The affinity matrix carries information about segmentation of the data — organization of mutual similarities between a set of data points. The dominant eigenvectors are used to perform the segmentation. Unlike K-means, spectral clustering can separate data into non-convex regions.

Anomaly detection has been used to detect changes in the behavior of jet engines on an aircraft, and to predict emerging failures in aviation systems. The anomaly detection methods described earlier need to be adapted to meet the requirements of SAO. For example, SAO requires the ability to check malfunction of the wireless spectrum, where anomalies could range from unwanted signal in a licensed band to the absence of the expected signal. The power spectral density data and autoencoder (a type of neural network) can been used to perform this function. A semi-supervised method could also be devised to detect changes to features like signal bandwidth, class and center frequency.

V. Cybersecurity Considerations for UAM Maturity Levels

The NASA concept of operations for UAM[24] describes passenger transport by electric Vertical Takeoff and Landing (eVTOL) aircraft in urban areas enabled by networked information technologies and air traffic management based on a service-oriented-architecture to provide communication, navigation, surveillance and cloud-based computing and software services. The FAA plans to play a regulatory role and delegate the responsibility of day-to-day operations to the Providers of Service to UAM (PSU). Several levels of maturity have been identified to calibrate progress in developing UAM because the growth of UAM depends on several interconnected factors such as advances in aircraft manufacturing, infrastructure development — vertiports and other facilities — traffic complexity, levels of automation and regulatory and societal acceptance. The UAM development is expected to go from the initial state to an intermediate state and finally to a mature state. Each state is divided into levels of UAM maturity Level (UML).[25-27] The traffic density, complexity of traffic and autonomy increases with each level. At UML-4, UAM will support simultaneous operations of hundreds of aircraft in urban environment, including in low visibility conditions, with some automation not requiring human intervention for safety. This stage of development assumes the system to be operationally ready, although not fully autonomous. UML-5 and UML-6 support an order of magnitude increase of traffic at each level with increasing levels of autonomy.

Security is a cross-cutting barrier to achieving NASA's UAM vision. The SAO must be designed to adapt to the changing CNSI infrastructure capability, and for meeting the needs of progressive levels of automation. The functions described below require secure communication of information between the participants. The FAA authorizes operations via an electronic identification (ID) that identifies the UAM aircraft (ownership, type and capabilities for example) by a unique code.[28] Entities with authorization will be able to exchange information with the PSUs, fleet operators and the FAA. Safety critical information such as position reports must be received wirelessly from nearby aircraft, and location of fixed obstacles need to be retrieved either from an onboard database or received wirelessly from a service provider for collision avoidance computations onboard the aircraft. Lower frequency planning and separation assurance information processed by the PSUs on the ground will be broadcast wirelessly to the aircraft. Communications will thus take place between aircraft and ground, ground-to-ground and aircraft-to-aircraft during flight. Aircraft ground operations and maintenance will need software updates and changes to their systems, which must be accomplished following security protocols. Dynamic changes to the airspace and routes will also require secure communications. The PSUs, which will maintain, process and distribute data to all the public agencies, should be trustworthy and available on demand.

Cybersecurity in UAM must extend and go beyond traditional information technology security procedures such as placing firewalls for restricting access to the network, and for preventing exposure of personal information. PSUs can be subjected to digital hijacking, cyberattacks, crypto key management and phishing attacks.[29-30] An operator might not share full information, which could cause another operator to make an erroneous critical decision for example regarding a conflict avoidance maneuver based on faulty information. The ability to change system behavior by malicious actors results in the requirement that the health of the system be continuously monitored using techniques such as continuous anomaly detection run on logged data. Additionally, cybersecurity in UAM must address security issues associated with automation that is increasingly dependent on sensors, networks and computer hardware and software for acquisition, distribution and processing of information. Critical automated systems often depend on information derived from GPS and ADS-B systems, which can be jammed. Failure of these systems can compromise the safety of UAM operations.

Security procedures can impose additional computational burden on the system. There can be a tradeoff between security and other safety critical functions especially when the computational resources are limited. Consider the

following example of conflict detection and resolution shown in Figure 5. The scenario shown in Figure 5 consists of (a) aircraft managed by PSU_A shown in red, (b) aircraft managed by PSU_B shown in blue and (c) aircraft managed by other PSUs or controlled by FAA shown in black. The aircraft operated by PSU_A and PSU_B are flying along the paths in the directions indicated by the arrows; the two paths intersect at right angles. The rectangles along the paths depict the separation between in-trail aircraft. To continue along their respective paths, aircraft X_A and X_B need to coordinate the order of entry into the common region along the two paths for ensuring separation between the aircraft. To determine separation, each aircraft will need to receive position reports from all aircraft in the vicinity — within the line-of-sight of its ADS-B-In receiver. Security stipulates that for every message received, the credentials of the sender be verified, and the payload of the message be examined for malicious content. A rogue aircraft or a transmitter on the ground could overwhelm the receivers with messages in a denial-of-service attack. Even if these malicious messages fail verification, and are discarded, the process of verification could add significant delay in processing messages from legitimate senders in safety critical situations. The amount of delay will depend on the algorithms used for verification, processing capability onboard UAM vehicles, UAM traffic density and other characteristics described in different NASA UMLs. Currently, standards for UAM cybersecurity do not exist; several organizations are in the process of developing them. Existing literature in vehicle-to-vehicle communication security for automobiles such as Ref. 31 might provide foundational information for the development of standards for UAM operations.

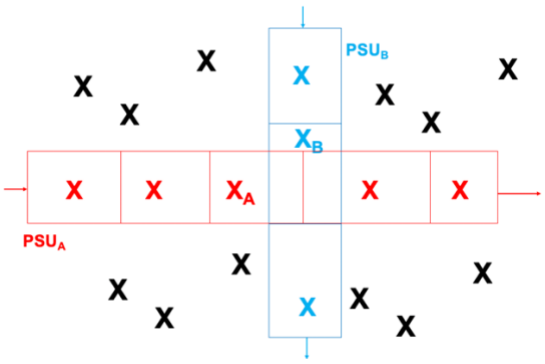

Figure 5. UAM traffic scenario

VI. Concluding Remarks

Unlike traditional aviation operations, Urban Air Mobility utilizes the CNSI infrastructure built for non-aviation applications and involves high level of automation as it matures. These two factors along with the evolving large number and complexity of UAM operations require a flexible and secure airspace system to support both normal and emergency operations of UAM. Aspects of the proposed Urban Air Mobility system concept were examined with the objective of identifying cyber security vulnerabilities. Wireless technologies and security issues of communications in mobile networks were discussed. Several methods for determining reliability of data — authenticity, accuracy, completeness and consistency of data — were briefly outlined. Cyber security technologies of Encryption, Blockchain, Virtual Information Fabric Infrastructure, Trusted Platform Module and Anomaly Detection for protecting the data were described. Finally, NASA's UAM maturity levels were briefly described, and the applicability of cybersecurity to its success was discussed.

References

[1]Committee, I. W., "ICAO working paper AN-Conf/13-WP/274," *13th Air Navigation Conference*, Montreal, Canada, 2018.

[2]Al-Falahy, N., & Alani, O. Y. (2017). Technologies for 5G networks: Challenges and opportunities. *IT Professional*, 19(1), pp. 12-20.

[3]Pokhrel, S. R., Ding, J., Park, J., Park, O. S., & Choi, J., "Towards enabling critical mmtc: A review of urllc within mmtc," *IEEE Access*, *8*, 2020, pp. 131796-131813.

[4]Sedgewick, A., "Framework for improving critical infrastructure cybersecurity," version 1.0, 2014.

[5]Rivest, R.L., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), pp.120-126.

[6]Diffie, W. and Hellman, M., 1976. New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), pp.644-654.

[7]Koblitz, N., 1987. Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), pp.203-209.

[8]Davis, R., 1978. The data encryption standard in perspective. *IEEE Communications Society Magazine*, *16*(6), pp.5-9.

[9]Touati, L., and Challal, Y., "Efficient cp-abe attribute/key management for iot applications," *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, IEEE, 2015, pp. 343–350.

[10]Yaga, D., Mell, P., Roby, N., and Scarfone, K., "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[11]S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. Accessed: Jan. 10, 2019. [Online]. Available: https://archive.is/rMBtV

[12]Reisman, R., "Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy," AIAA-2019-2203, 2019 AIAA Science and Technology Forum (SciTech), San Diego, CA, 7-11 Jan. 2019.

[13]G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, vol. 151, Apr. 2014, pp. 1-32.

[14]S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake,"' Tech. Rep., Aug. 2012. Accessed: Jan. 10, 2021.

[15]E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," *13th EuroSyst. Conf.*, 2018, pp. 30.

[16]D. Joshi, "IBM, Amazon & Microsoft are offering their blockchain technology as a service," *Bus. Insider*, vol. 24, Oct. 2017. Accessed: Jan. 10, 2019. [Online]. Available: https://www.thewealthadvisor.com/article/ibm-amazon-microsoft-are-offering-theirblockchain-technology-service

[17]Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., and Wang, F.-Y., "An overview of smart contract: Architecture, applications, and future trends," *IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 108-113.

[18]Brandenburger, M., Cachin, C., Kapitza, R., and Sorniotti, A., "Blockchain and trusted computing: Problems, pitfalls, and a solution for hyperledger fabric," 2018. [Online]. Available: https://arxiv.org/abs/1805.08541

[19]Kuo, T. T., Zavaleta Rojas, H., and Ohno-Machado, L., "Comparison of blockchain platforms: a systematic review and healthcare examples," *Journal of the American Medical Informatics Association*, 26(5), 2019, pp.462-478.

[20]Elshambakey, M., Khalefa, M., Tolone, W. J., Bhattacharjee, S. D., Lee, H., Cinquini, L., Schlueter, S., Cho, I., Dou, W., and Crichton, D. J., "Towards a distributed infrastructure for data-driven discoveries & analysis," *2017 IEEE International Conference on Big Data (Big Data)*, IEEE, 2017, pp. 4738–4740.

[21]Hoeller, A. and Toegl, R., "Trusted platform modules in cyber-physical systems: On the interference between security and dependability," *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, April 2018, pp. 136-144.

[22]Friedman, J., Hastie, T. and Tibshirani, R., "The elements of statistical learning," *New York: Springer series in statistics*, vol. 1, no. 10, 2001.

[23]Ng, A. Y., Jordan, M. I. and Weiss, Y., "On spectral clustering: Analysis and an algorithm," *Advances in neural information processing systems*, 2, 2002, pp.849-856.

[24]Thipphavong, D. P. et.al., "Urban Air Mobility Airspace Integration Concepts and Considerations," *18th AIAA Aviation Technology, Integration, and Operations Conference*, Atlanta, Georgia, June 25-29, 2018.

[25]Price, G., Douglas, H., Kyle, J., Mike, K., Steve, P., and Russell, W., "Urban Air Mobility Operational Concept (OpsCon) Passenger-Carrying Operations," NASA/CR-2020-500158, May 2020. https://ntrs.nasa.gov/citations/20205001587, accessed November 18, 2020.

[26]Deloitte, NASA, "UAM Vision Concept of Operations UAM Maturity Level (UML)-4 Version 1.0," NASA/TM-2020-000000, Washington, DC.

[27]Verma, S. A., Monheim, S. C., Moolchandani, K. A., Pradeep, P., Cheng, A. W., Thipphavong, D. P., and Wei, B., "Lessons learned: using UTM paradigm for urban air mobility operations," *AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, October 2020, pp. 1-10.

[28]"The FAA Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations version 2 (UTM ConOps)," March 2020.

[29]National Academies of Sciences, Engineering, and Medicine, "Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System," *The National Academies Press*, Washington, DC, 2018.

[30]National Academies of Sciences, Engineering, and Medicine, "Advancing Aerial Mobility: A National Blueprint, Prepublication Copy," *The National Academies Press*, Washington, DC, 2020.

[31]Baee, M. A. R., Simpson, L., Foo, E., and Pieprzyk, J., "Broadcast Authentication in Latency-Critical Applications: On the Efficiency of IEEE 1609.2," *IEEE Transactions on Vehicular Technology*, 68(12), 2019, pp. 11577-1158.