https://doi.org/10.7840/kics.2023.48.8.984

Consideration of Cybersecurity threat for Urban Air Mobility (UAM) Operations

Sanghoon Jeon◆

ABSTRACT

Urban air mobility (UAM) is rapidly becoming an alternative to traditional ground transportation, owing to the development of hyper-connected communication technology. However, safely transitioning from ground transportation to an air transportation system requires research in various fields. To ensure safe and efficient urban flight management, the operation of air and passenger transportation services requires the integration of various technologies and regulations across multiple fields. This includes safe operations for aircraft, vertiports and air control centers in the physical domain, and information security technology operations for cybersecurity in the cyber domain. As UAM systems become increasingly reliant on connected technologies and data, effective countermeasures against cybersecurity threats are essential for ensuring their safe and secure operation. This could involve implementing robust cybersecurity protocols and leveraging advanced anti-threat technologies to identify and respond to potential threats. However, urban aviation operations face unique potential threats that are not typically encountered by general aircraft services. These include interference from ground operations, sabotage, exposure of aviation information, interception, tampering, theft, and fraudulent use. Moreover, vulnerabilities in the operation and management of manned and unmanned aircraft, pilots, remote pilots, vertiports, and air traffic control centers can be exposed and exploited. Therefore, this study aims to identify potential threats and vulnerabilities associated with UAM operations, and propose security requirements and reliable countermeasures to ensure their safe and secure operation against cyber threats.

Key Words : Urban air mobility, UAS, Operations, Authentication, OCSP

Ⅰ. Introduction

With the development of hyper-connected communication technology, ICT has evolved by integrating various fields, such as automobiles and aviation. The development of mobile communication technologies, such as 5G and 6G, helps alleviate ground traffic congestion and transport or move people or cargo between places (regions, within regions, cities, etc.). Consequently, research is being conducted on low-altitude mobile communication technology for transporting people or cargo to areas where air services are insufficient. Furthermore, it is advancing toward the demonstration stage of developing Urban Air Mobility (UAM) services. UAM is expected to revolutionize urban transportation as a faster, greener, and more efficient alternative to traditional ground transportation.

However, the safe conversion of ground transportation systems into air transportation systems through UAM requires extensive research across various fields, including aerodynamics, materials science, control systems, propulsion technology, air traffic management, and human factors[1-5]. Ensuring safety in air transportation technology necessitates technological convergence and regulation across various technical fields, including aerodynamics, materials science, control systems, and propulsion

◆ First Author : Far East University Department of Hacking & Security, randyjeon@gmail.com, 정회원
논문번호 : 202305-098-C-RU, Received May 12 2023; Revised June 5, 2023; Accepted June 7, 2023

technology. Additionally, to safely manage the increasing air traffic volume in the future, it is necessary to establish regulations and safety standards that ensure the safety of passengers and crew, covering areas such as air traffic control, pilot training, and maintenance.

To develop a safe and efficient urban air mobility service, various studies are required, including a thorough understanding of the technical aspects of aircraft, airspace regulations, and security protocols. To ensure the efficient operation of the air traffic management system (ATC) and vertiport infrastructure, it is necessary to address the unique requirements of high-density batteries and propulsion systems, as well as ensure safe and reliable flight and air traffic management in various traffic conditions. This includes developing systems that can manage cybersecurity risks and implement robust protocols for data protection, threat detection, response, and access control. Various studies are underway to explore alternative forms of transportation to replace traditional means, such as Unmanned Aerial Vehicles (UAV), Personal Aviation Vehicles (PAV), and UAM systems. These technologies are being developed to improve the efficiency, safety, and environmental impact of transportation, and could have a transformative impact on urban mobility in the future. Effective regulations and operational frameworks must be established for urban air traffic services, considering the specific type of service, intended purpose, and use of aircraft systems. This requires careful consideration of factors such as safety, efficiency, and environmental impact, as well as collaboration between industry stakeholders, regulatory bodies, and local governments.

Despite technological advancements in aircraft for current services (including both manned and unmanned aircraft), regulations, technical standards, and operational technologies have not yet been adequately developed. For example, there is a lack of standardization in security technology and other measures to mitigate potential threats such as interference with aircraft operation, obstruction, exposure of aviation-related information, interception, counterfeiting, falsification, and theft by unauthorized individuals. Additionally, the use of high-speed communication networks and security technologies for low-altitude navigation needs to be defined.

This study proposes considerations for cybersecurity from the perspective of UAM operations. Chapter 2 covers the considerations related to UAM in the current demonstration stage, whereas Chapter 3 discusses the potential threats and vulnerabilities of the operations. Chapter 4 presents the considerations and security requirements for UAM operations, and Chapter 5 concludes with the proposed operation method for cybersecurity.

Ⅱ. Related works

2.1 Considerations for UAM and unmanned aerial systems (UAS) Services

UAM was first developed in the early 2000s as a privately owned small-class aircraft called a PAV, which later evolved into a road-capable aircraft capable of conventional take-off and landing (CTOL), short take-off and landing (STOL), or vertical take-off and landing (VTOL), depending on the runway length. This form of air mobility uses various power sources such as internal combustion engines, secondary batteries, solar cells, and electricity. They are also known by various names, such as flying cars, drone taxis, air taxis, vertical takeoff and landing aircraft, and personal aircraft. As remotely controlled unmanned aerial vehicles continue to develop, urban air mobility is being explored for various uses, purposes, and service types, including drones, as a means of transportation and UAS (Figure 1)[6].

However, the absence of standards and guidelines for airworthiness certification, regulations, general matters, operation methods, and flight security guidelines for manned and unmanned urban air mobility services has caused confusion in the operation and communication between aircraft, air traffic control systems, and vertiports. This has resulted in operational interference and obstruction of city aircraft, as well as exposure of aviation-related information to potential threats, such as interception, forgery, alteration, and theft.

Therefore, there is an urgent need to develop

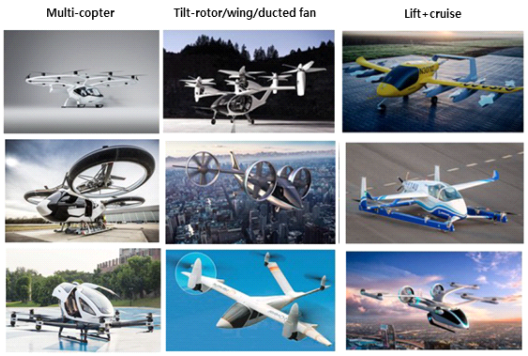

Fig. 1. Types of Personal Air Vehicle (PAV)

countermeasures. Despite ongoing research on unmanned autonomous flights using drones and UAM as a means of transportation, several issues must be considered during their operation, including the following:

Airworthiness certification. They must meet certain safety standards before being certified for flights. This includes ensuring that these flights are built using quality materials, have proper maintenance schedules, and are equipped with adequate safety features.

Remote pilot qualification certification. Operators must be properly trained and certified to ensure that they have the necessary skills for safe operation.

Certification/verification. Unmanned aircrafts must be certified and verified to ensure that they meet the required standards for airworthiness and safety.

Fraudulent use. There is a risk of malicious purposes such as terrorism or espionage. This highlights the need for security measures to prevent unauthorized access.

Security guidelines. Security guidelines are required to ensure secure communication between Traffic Management systems and UAM. The transmission and reception of CNSI (Communication, Navigation, Surveillance, Information) must be secure to prevent unauthorized access.

Additionally, the accessibility of UAM services depends largely on the availability of suitable takeoff and landing sites. To this end, researchers have explored the use of helipads, such as landing pads or vertiports, in buildings in city centers or existing structures. Different organizations have proposed various standards for the dimensions of the helicopter landing area, such as the Final Approach and Take-Off area (FATO), Touchdown and Lift-Off area (TLOF), Safety Area (SA), Ground Taxiway, and parking lots. For instance, in the case of helicopters, the International Civil Aviation Organization (ICAO), the Federal Aviation Administration (FAA), Uber, MIT, and K-UAM (Korea) have suggested different standards for FATO, such as 1D (full-length or full width) for ICAO, 1.5D for FAA, 75 ft for Uber, and 1.5D for MIT (68 ft ≒ 21m), while K-UAM proposes a standard of 1.5D. Table 1 shows the installation standard amendment[7].

However, different organizations, including the ICAO, FAA, K-UAM (Korea), private companies, and research institutes, have proposed various standards for airfields (or buildings) to support services. Common installation and service standards that can be applied across regions and countries are required to ensure interoperability and safety. It is essential to distinguish between airfield installation standards for unmanned aerial systems and those for urban air mobility, including the mixed use of airfields or existing helipads. Moreover, the lack of operational security guidelines is an urgent issue that must be addressed.

Table 1. Installation standard amendment

Types	ICAO Helicopter	FAA Helicopter	Uber UAM	MIT(45ft) UAM	K-UAM (KOREA) K-UAM
FATO	1D	1.5D	75ft	1.5D(68ft ≒21m)	1.5D
TLOF	0.83D	1RD	50ft	1D(45ft ≒15m)	1D
SA	0.25D (or 3m)	0.3~0.5D	-	26ft(20ft ≒6m)	20ft
Ground Taxiway	1.5UCW	2UCW	-	1.5D	1.5D
Aircraft stand	1.2D ~more	1.5RD	-	1D	1D

Source : ICAO, FAA, "System analysis of UAM operation scaling"(MIT ICAT), "Here's how Uber is designing Skyport for future air taxis(2020)"(Aviation today).

2.2 Potential cybersecurity threat of UAM service network

UAM services have been investigating the use of commercial mobile communication networks (such as 5G and 6G) for low-altitude air control and operations.

Table 2 lists the communication technologies considered to provide air mobility services. In its ongoing urban air mobility service demonstrations, CNSi has expanded its commercial mobile communication network for control and management at low altitudes [7].

However, multiple communication networks, including commercial mobile communication networks, C2, and low-orbit mobile communications,

Table 2. Communication types and Usages

Communication technology	Descriptions
ADS-B	This type of communication is used for air traffic control by broadcasting its position information to other aircraft and ATC using VHF bandwidth.
GNSS	This type of communication is the worldwide positioning, navigation, and timing determination capability available from one or more satellite constellations.
Wi-Fi	This type of communication is used for providing broadband services in a cabin through SatCom or a cellular network.
SatCom	This system provides broadband services in the cabin of aircraft by using satellite communication channel.
V2V	This type of communication is used for aircraft-to-aircraft communication to share information and prevent collision between aircraft using the cellular network.
C2(Command and control)	The data link between the remotely-piloted aircraft and the remote pilot station for the purposes of managing the flight.
Cellular	These types of communication are used for providing broadband services in the cabin of aircraft and command & control communication by using cellular network channels.

are being utilized. Despite these efforts, several vulnerabilities have been identified in commercial mobile communication networks[9]. These expose subscriber information to collection by fake device stations, with concerns regarding the confidentiality and integrity of control traffic.

5G offers advantages over 4G in terms of providing more secure communication services by encrypting subscriber identifiers and using the TLS for the transmission and reception of information. However, potential vulnerabilities and threats still occur when switching between 4G and 5G networks. There is a potential threat of “downgrade attacks” when switching between these networks, where attackers force the use of a less secure network (e.g., 4G) to intercept or manipulate traffic. Additionally, although network slicing technology using SDN/NFN can enhance security, it is not foolproof, and potential errors and vulnerabilities due to interference between slicing still exist. Countermeasures must be developed and implemented to mitigate potential security risks. Additionally, although security is being strengthened using network slicing technology with SDN/NFN, potential errors and vulnerabilities due to interference between slicing still exist, and countermeasures have not been proposed.

Ⅲ. Considerations from the perspective of UAM operation and potential cyber threats

3.1 Potential cybersecurity threat of UAM service network

UAM, which is currently in the demonstration stage, is being developed alongside unmanned aerial systems to transition from a conceptual mode of transportation to a widespread ground and air transportation method. Automation technology is the foundation for the safe operation of both manned and unmanned aircraft. To integrate into multi-modal transportation systems, security operations must be implemented for passengers and cargo to protect against malicious activities, such as fraud and denial of service attacks. Additionally, operational vulnerabilities must be addressed. Furthermore, security technologies suitable for the evolving

communication technologies should be applied. The most crucial service is to address the vulnerabilities of commercial mobile communication networks (highlighted in Section 2.2).

Thus, as communication technology advances, it is crucial to ensure the security, integrity, and availability of operational information, including autonomous and semi-autonomous control technologies, communication information, and operational data. According to the current operation guidelines, a draft operation procedure is prepared by dividing the flight into several stages, including flight planning, pre-flight, taxiing and takeoff, climb and cruise, approach and landing, taxiing, and operational stages after stopping, following traditional aviation operation methods.

However, this procedure does not ensure safety against threats that can interfere with the flight. For instance, during the flight stages of takeoff, ascent, cruise, and landing, UAM is exposed to potential threats, such as collisions, interference with UAS, or unauthorized drones. While manned aircraft operations allow pilots to respond to unexpected situations, unmanned aircrafts, such as UAS or drones, operate on unmanned or remote automatic flights, making it necessary to prepare countermeasures against potential threats, such as collisions or interruptions caused by denial-of-service attacks. Moreover, during operation, communication security methods for the secure exchange of flight information between ground control centers, such as vertiports, air traffic control, and traffic management service providers, must be strengthened. The corridor is vulnerable to potential threats such as the intrusion of unauthorized aircraft, hijacking aircraft, and falsification/forgery of flight information.

As a result, real-time authentication and verification technology are required for pilots or aircraft operating UAM within the corridor, as well as the UAS.

3.2 Necessity and standardization of UAM integrated operation design

Various airframes such as drones, unmanned aerial systems, and UAM systems have been developed and researched for advanced air mobility (AAM) services, with significant progress in autonomous flight technologies.

AAM operation areas can be classified into UAS (piloted and unmanned automated areas) and UAM. All UAV must be registered according to the International Civil Aviation Organization (ICAO) regulations. UAV weighing 25 kg or less and operating under standard conditions do not require additional operational review.

However, license and identification module technology and the development of standard technology related to communication protocols, drone authentication, and encrypted communication are not currently ongoing[10,11].

In ITU-T SG17, security guidelines are being developed for connected electric vertical takeoff and landing (eVTOL) vehicles in UAM environments. However, these guidelines have limited consideration for software, and do not cover security considerations on the operation side[8].

According to ISO TC 204, Intelligent transport systems (ITS) are working on the standardization of combined transportation, commercial transportation, traffic management, emergency services, and commercial services in the field of intelligent vehicles (artificial intelligence, autonomous driving, etc.). TC 204 is working on the standardization of information, communication, and control systems in urban and rural ground transportation. However, UAM Operation security guidelines for cybersecurity have not yet been developed[12,13].

ISO/IEC JTC 1/SC 17 WG12 is working on standardizing the drone license and identification module technology. The development of standard technologies related to communication protocols, drone authentication, and encrypted communication for drones is ongoing[14].

As such, different technical standardizations are implemented in different organizations. For AAM services, common convergence technology standardization must be performed. Without standardization, it causes confusion in the operation and communication between aircraft, vertiports, and air traffic control centers as well as operation

interference, obstruction, collision, fraudulent use, exposure of aviation-related information from unauthorized persons, interception, tampering, and stealing.

The integration of UAM and UAS is expected to lead to the development of AAM, which could potentially replace current ground transportation. To ensure safe and secure operations of both manned and unmanned cargo and passenger transport, integrated operational guidelines and regulations are required. This includes the development of operational regulations and security technology to ensure the safe and secure operation of UAM, UAS, and drones.

Ⅳ. Consideration of cybersecurity for securing UAM operations against cyberthreats

Along with the development of communication technology, UAM services aim to provide AAM services, such as manual, semi-autonomous, and autonomous flight of manned (and unmanned) aircraft, along with unmanned aerial systems services as an alternative means of traditional transportation. Research and development at the demonstration stage are currently underway. To ensure secure and efficient operations against cyberthreats, several factors must be considered.

Airspaces integrated operation. The airspaces of the UAM, UAS, and drone are highly differentiated, but each airspace must be operated and managed in an integrated manner to avoid collisions with other aircraft by forced navigation, and ensure safety.

Infrastructure. The services require dedicated landing and take-off areas, such as helipads or vertiports, which must be designed and maintained to ensure secure communication and accessibility for passengers and operators from cyber threats, such as intercepting communication.

Air Traffic Management (ATM). ATM systems must be capable of handling increasing traffic and providing secure and efficient routing, coordination, and communication between operators and air traffic controls.

Cybersecurity. These services rely on digital technologies that are vulnerable to cybersecurity threats. Robust cybersecurity measures should be implemented to prevent unauthorized access, data breaches, and other security incidents.

Regulations. Regulations and standards must be developed to govern operations, including cybersecurity, safety, certification, and licensing requirements.

Considering these factors, airspaces intergrated operation, infrastructure, ATM and regulations must be developed and operated safely, efficiently, and sustainably. Reliable navigation information is required to safely operate multiple aircrafts sharing the same airspace. The flight system must ensure accuracy, integrity, availability, and continuity of information.

Establishing a trustworthy accredited certification body such as an air traffic control system can provide security functions such as confidentiality, availability, integrity, authentication, access control, and non-repudiation. This ensures that only certified and verified aircraft, pilots, and remote pilots can fly and operate using the PKI-based method, thus mitigating potential cyber threats and enhancing security. Current mobile communication networks can increase availability and efficiency.

The aviation control center (ATC) issued IC card-based certificates to verify the credentials of aircrafts, pilots, and remote pilots. For the PKI-based X.509 certificate, a certificate issued by Sign Korea was used, which was applied to the UAM, pilot, and system. An Online Certificate Status Protocol (OCSP) server that verifies the status of each certificate was constructed and tested.

The OCSP server test environment was built using Red Hat Enterprise Linux Server release 7.8 (Maipo), Intel(R) Xeon(R) Gold 6244 CPU @ 3.60GH system. Figure 2 shows the real-time verification of UAM or pilot's X.509 certificates using the OCSP [15-18], which allows for quick and reliable certificate status checks. Real-time verification is possible using the OCSP (Figure 2).

Figure 2 illustrates the process of authenticating and verifying a user through certificate validation. This is achieved by verifying the X.509 certificate issued by a trusted domestic certification authority using an OCSP test server.

By leveraging the advantages of PKI-based

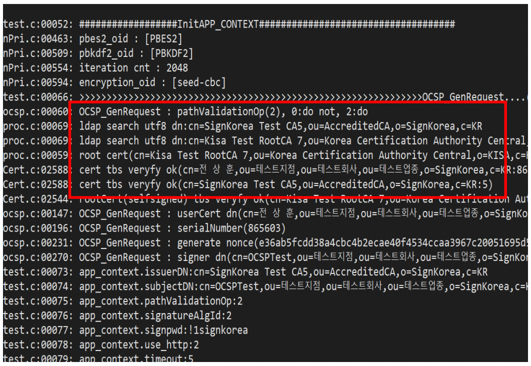

Fig. 2. Verification of real-time certificate status by Online Certificate Status Protocol (OCSP)

technology, including authentication prevention, multisession prevention, and interception prevention, security can be enhanced by storing certificates on IC cards. Furthermore, by conducting a real-time verification of user certificates, the availability of certificate users can be confirmed. Table 3 presents the results of the experiments that tested the effectiveness of this verification method in ensuring security, authentication, availability, and other factors. The experiments confirmed that the use of X.509 certificates and OCSP strengthened security against cyber threats, such as DDoS and replay attacks.

Table 3. Proposed method improvement effect

Classification	Descriptions	Effectiveness
Security	Key inference and prevention of exposure, information encryption through strong SOD and 5G encryption technology	Confidentiality and fraud prevention
Authentication	Real-time member (aircraft, pilot, system, etc.) operator mutual authentication	In flight, mutual authentication
Re-attack responsiveness	Physical and logical system access control through conditional access control of unique identifiers	Access control
Availability	Enhanced and automated real-time authentication/ verification with unmanned aerial vehicles and autonomous flight	Increase availability
Connection security and persistence	Respond to re-attacks through real-time certificate verification	User authentication and validation

Ⅳ. Conclusions

This study discusses the potential threats and vulnerabilities of upcoming UAM services, and proposes security requirements in both the physical and cybersecurity domains. It emphasizes the need for reliable navigation technology and information exchange for collision avoidance as aircraft autonomy increases.

Additionally, for safe UAM operations, PKI-based technology is used to verify users (UAM aircraft, pilots, each system, and system operator) in advance, thereby strengthening operational safety, security, and availability to prevent cyber threats. Countermeasures for implementation are also suggested.

To contribute to the safe and stable provision of UAM services, we plan to continue research on mutual authentication and verification technologies to further enhance the safety and security of UAM operations.

References

[1] Ministry of Land Infrastructure and Transport, *K-UAM Technology Roadmap*, 2021.

[2] UAM Team Korea, *K-UAM Concept of Operation 1.0*, 2021.

[3] FAA, "*Urban Air Mobility (UAM) Concept of Operations v1.0*," 2020, https://nari.arc.nasa.gov/sites/default/files/attachments/UAM_ConOps_v1.0.pdf (accessed on 07 April 2023).

[4] NASA and Deloitte, *UAM Vision Concept of Operations (ConOps) UAM Maturity Level(UML) 4*, 2020.

[5] EMBRAER, *Urban Traffic Management Concept of Operations (Version 1)*, 2020.

[6] KISTEP, *Personal Air Vehicle (PAV)*, 2021.

[7] ICAO, FAA, "*System Analysis of UAM Operational Scaling*" *(MIT ICAT)*, "*Here's How Uber Is Designing Skyports for Future Air Taxis(2020)*" (Aviation today).

[8] *Xevtol-sec: Security guidelines for an electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment*, ITU-T, 2023.

[9] S. R. Hussain, et al., “Privacy attacks to the 4g and 5g cellular paging protocols using side channel information,” *NDSS Symp. 2019*, Feb. 2019.

[10] ICAO, *Unmanned Aircraft Systems (UAS) [25 kilograms or less] Operating in compliance with [Part 101] Rules.*

[11] ICAO, *ICAO MODEL UAS REGULATIONS Part 101 and Part 102*, Jun. 23, 2020.

[12] ISO/TR 23629-1:2020, *UAS Traffic Management (UTM)— Part 1: Survey results on UTM.*

[13] ISO/DIS 23629-8, *UAS Traffic Management (UTM) — Part 8: Remote Identification.*

[14] ISO/IEC WD 22460-2:2021, *Cards and security devices for personal identification-ISO License and Drone Identity Module.*

[15] ISO/IEC 7816-8:2021, *Identification cards-Integrated circuit cards-Part 8: Commands and mechanisms for security operations.*

[16] ISO/IEC 27099:2022, *Information technology-Public key infrastructure-Practices and policy framework.*

[17] RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol.*

[18] S. Jeon, “Mutual Authentication Method for Secure UAM Operation Based on 5G Network,” *The Soc. Convergence Knowledge Trans.*, vol. 11, no. 1, 2023.

전 상 훈 (Sanghoon Jeon)

Apr. 2021~Current : Professor, Far East University, Department of Hacking & Security.

Dec. 2010~Current : ISO/IEC JTC1/SC27 WG4, Head of Delegate-Korea

Feb. 2019~Current : IUT-T SG17 (Security) Delegate

<Research Interests> Information Security, Aviation Security, Network Security, Entity Authentication

[ORCID:0000-0002-5365-3174]