Security Strategies for Unmanned Aircraft Systems Networks

Marco Hernandez*†, Gürkan Gür‡, Kamesh Namuduri§

* Center for Wireless Communications, Oulu University, Finland
† Yokosuka Research Park-International Alliance Institute (YRP-IAI), Japan
‡ Zurich University of Applied Sciences (ZHAW), Switzerland
§ University of North Texas, USA

marco.hernandez@ieee.org, gurkan.gur@zhaw.ch, kamesh.namuduri@unt.edu

***Abstract*—The rapid growth of Unmanned Aircraft Systems (UASs) usage in both commercial and defense areas has increased the requirement for advanced security schemes for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications for UASs. We define a UAS as consisting of a Control Station (CS) on the ground and at least one UAV. The pilot in the CS may have Visual Line-of-Sight (VLOS) or may not have VLOS to the airborne UAVs. The integration of UASs into the National Airspace (NAS) will rely on Unmanned Traffic Management (UTM) systems which can support Detect-And-Avoid (DAA) and de-confliction of flight paths. In case of non-cooperative traffic, tactical (in-flight) deconfliction becomes a critical element. In Beyond Visual Line of Sight (BVLoS) operations, where a remote pilot is unable to visually monitor the airspace beyond LoS, Sense-and-Avoid strategies become necessary. Further, the communication devices and messages must be protected against hacking and cyber-attacks. This paper investigates several use cases for UAS-to-UAS or V2V operations for UASs and the cyber-security strategies for protecting V2V communications addressed by IEEE P1920.2, a new standard for V2V communications for UASs, currently under development. This discussion included authentication of V2V parties, protection of Remote ID, cryptographic key management, and authorization policies based on a zero-trust architecture.**

***Index Terms*—UAV networks, security, IEEE P1920.2, zero trust architecture, security management.**

I. Introduction

The IEEE P1920.2 Working Group (WG) is in the process of developing Vehicle-to-Vehicle (V2V) communications standard for Unmanned Aircraft Systems (UASs) [1]. This standard includes a protocol and a format for exchanging information among UASs, and is agnostic to radios and spectrum. A UAS is assumed to include a Unmanned Aerial vehicle (UAV), its command and control (C2) unit, Ground Control Station (GCS), and a remote operator or pilot [2]. The information exchanged between a UAS with other UASs and GCS includes C2, telemetry, navigation safety messages such as Detect-And-Avoid (DAA), and application-specific data information for applications in Visual Line of Sight (VLoS) and Beyond Visual Line of Sight (BVLoS), but, with a direct radio link between GCS and UAS. BVLoS refers to the scenario in which a UAV is not in VLOS from the GCS. BRLOS refers to the scenario in which a UAS is not in VLOS and without a direct radio link from the GCS, suggesting the need for an intermediary relay radio link as depicted in Fig. 1. BRLOS situations are present in hilly terrains and urban areas where radio waves may be blocked [3].

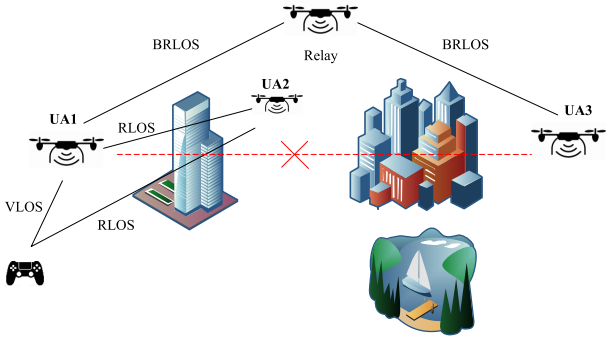

Fig. 1. V2V operational environment.

This paper outlines the progress made so far by the IEEE P1920.2 WG in developing the V2V communication standard. The main contributions of this work are two-fold: First, it delineates a set of potential use case scenarios in which V2V communications among UASs play a critical role and essentially require security mechanisms. These use cases were gathered from several sources including the Radio Technical Commission for Aeronautics (RTCA) [4], and two white papers produced by IEEE and General Aviation Manufacturers Association (GAMA). Secondly, security vulnerabilities, and strategies for protecting communications between UASs are presented and discussed.

The rest of the paper is organized as follows: Section II describes potential use case scenarios. Section III outlines the security vulnerabilities. Section IV presents the threat model. Security and trust model is outlined in section V. Section VI outlines the UAS security management framework. Section VII presents the zero trust architecture for UAS networks. Section VIII discusses data security. Finally, conclusions are

DOI: 10.1109/ICCWorkshops57953.2023.10283520

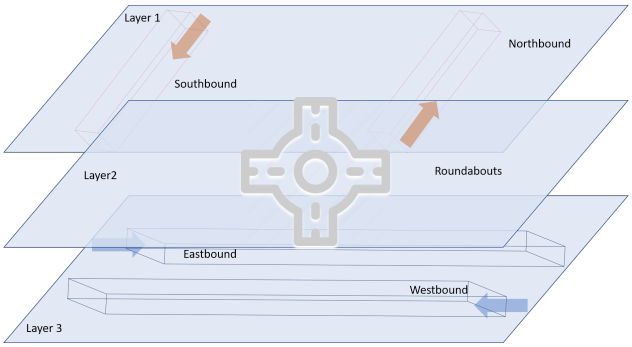

Fig. 2. An illustration of roundabout or circular intersection in an air corridor

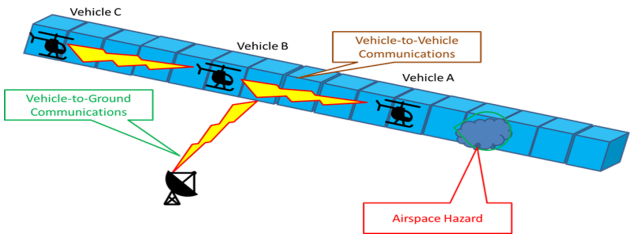

Fig. 3. Illustration of airborne separation in a skylane

presented in Section IX.

II. Potential Use Case Scenarios

This section outlines potential scenarios that the task group currently consider developing. These scenarios are based on the suggestions that came from a meeting organized by the Radio Technical Commission for Aeronautics (RTCA) in September 2022 [4]. The five use cases support the airspace operations in Advance Air Mobility (AAM) ecosystem.

1) Collision Avoidance: In this case, two or more UASs are approaching a region at the same time and they need to avoid a potential collision. There can be many variations to this scenario. For example, the vehicles can be cooperative or non-cooperative [5]. The airspace can be structured or unstructured. Structured airspaces are defined and reserved for certain types of vehicles and typically applicable for urban areas. Unstructured airspaces are typical for rural regions.
2) Merging and Spacing/Sequencing of Traffic: This use case refers to traffic in structured airspaces, i.e., air corridors. An air corridor is a highway system in the airspace. Air corridors are reserved airspaces at altitudes ranging from 150 meters to 1 kilometer Above Ground Level (AGL) [6]. Imagine an intersection such as a roundabout illustrated in Fig. 2. Merging occurs when a UAS is trying to enter the roundabout.
3) Airborne Separation: This scenario refers to the need for maintaining a safe distance between any pair of UASs during flight. Two situations arise depending on whether UASs are flying in structured or unstructured airspace. The former case is illustrated in in Fig. 3. Here, if the UAS in front decelerates, the vehicle behind it needs to decelerate as well in order to maintain a safe distance between the two. In the later case, each UAS assumes a geofence [7] around it in order to maintain a safe distance from other UASs.
4) Airborne Rerouting: Rerouting of a UAS may be needed when the planned or current route is not navigable due to airspace space hazards such as the one shown in the Fig. 3. Typically, the new route is shared with the UAS by the remote operator (pilot) on the ground or by the Ground Control Station (GCS) if the UAS is within the communication range of the operator or GCS. If the UAS is Beyond the Radio Line-of-Sight (BRLSO), the rerouting information may be relayed by one or more UASs. Rerouting may also be required when a vertiport where a UAS planned to land becomes unavailable. In this case, the UAS needs to to change its destination to another available vertiport that is close by. These scenarios also emphasize the need for a multi-hop connection or UAS network for sharing mission critical information in real-time.
5) Weather/winds: Sudden weather development during a flight might require a UAS to reroute its planned flight path as in the previous scenario. In extreme weather conditions a UAS may need to land in a nearby location or return home immediately. In such situations, the weather information and the message indicating immediate landing need to be delivered to the UAS.

III. Security vulnerabilities in UASs

UAVs have a unique characteristic security-wise. Unlike PCs, personal devices o servers, UAVs in V2V configurations (unicast, multicast, or broadcast) are unprotected by Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) systems, leaving them vulnerable to cyber-attacks [8]. Since an attack can precipitate a life-and-death event, or propagate to other UAV systems or infrastructure, the magnitude of the impact is considerably important. Because of this unique security profile, UAVs, especially in V2V configurations, require a different approach. These are reflected in the use cases described in Section II.

The following characteristics are unique to UAVs:

- Small UAVs have limited resources in terms of energy consumption and computational processing, making it harder to secure them or apply monitoring and protection.
- Conventional cyber-security solutions are too computationally intensive for the low power, limited battery life, and memory capacities of UAVs.
- Unlike PCs or personal devices, the different components of UAVs are updated infrequently. UAVs rely heavily on third-party libraries and components. Releasing a patch may be organizationally difficult and left to users to check

by themselves for updates. When updates are released, components may remain unpatched, leaving UAVs vulnerable to attacks.

- UAVs have many types of hardware that include diverse operating systems, from different flavors of Linux to real-time operating systems. The same for the firmware that controls the radio interfaces: telemetry, command and control, communications, and GPS (as well as sensors and actuators). Together they create a large attack surface with a wide range of different vulnerabilities.

Hence, UAS vulnerabilities stem from various factors:

1) Inadequate policies and procedures to develop and maintain hardware and software UAS platforms.
2) Inadequate designed UAS networks with insufficient defense and security protections.
3) Remote access without appropriate access control policies and authentication.
4) Inadequate secured wireless communication protections.
5) Lack of tools to detect anomalous activity.

IV. Threat model

IEEE 1920.2 considers both passive attacks and active attacks. A passive attack aims to learn or use information extracted from the target system, but does not affect that system's operation. An active attack attempts to alter the system's resources or affect its operations.

In this context, the pertinent cyber threats include:

1) Spoofing of civil GPS and Remote ID signals as those are transmitted in the clear (not protected against passive or active attacks) and publicly available.
2) Jamming communication links (GPS, Remote ID, C2, DAA, data communications).
3) DoS attack: It targets the UAS availability by exhausting the network bandwidth. Either by flooding the system with spurious packets or by continuously sending known commands or control signals disrupting system services. Also, DoS may occur by jamming communication links.
4) Eavesdropping on command & control, data communications, or telemetry signals.
5) Intercept and alter command & control, data communications, GPS, or Remote ID signals.
6) The Federal Aviation Administration (FAA) in the US requires Remote ID and Automatic Dependent Surveillance-Broadcast (ADS-B) messages to be transmitted in the clear (unsecure) to make them available to personal devices. Conventional encryption-based approaches are not workable solutions because of such regulatory constraints. Therefore, a key challenge is how to develop and integrate efficient countermeasure methods against various attacks while considering the existing infrastructure and protocols [9].
7) GPS dependence: Operation and navigation of UAVs are highly dependent on GPS. This dependency makes UAVs navigation very difficult when GPS signals are not available due to a DoS attack (like jamming) or trusted due to injection of spoofed GPS signals.
8) Another security risk is related to the impact of cyber-attacks on other subsystems such as sensors, cameras, etc. Attacks on these subsystems can make them malfunction, which can cause failure in the UAS operation, from draining the battery faster to changing the flight path.

A compromised UAS platform can be a point of attack on infrastructure (cellular network, Wi-Fi access point) when connected or provoke an accident. Public safety is of paramount importance and consequently the implementation of security mechanisms by IEEE 1920.2 to protect UAS from cyber-attacks. Securing UAS is more challenging than other communication or computer networks because of the disparity in subsystems, network mobility, and diversity of data flows C2, DAA, and data (video, audio, or image).

Current UAS platfoms supports weak security protections or nothing at all. As a result, a UAS may be the target of cyberattacks including unauthorized connections, illegal access, malicious intent to sabotage the operation of the UAS network or being a point of attack on infrastructure.

V. Security and trust model for IEEE 1920.2

Except for physical threats such as jamming, the threats mentioned above can be prevented by the proposed security protocol with the following capabilities:

Mutual entity authentication Data origin authentication for sender and receiver.

Mutual explicit key agreement authentication Mutual explicit key authentication is the property obtained when the sender and receiver have the assurance that only the other party knows the negotiated shared key.

Confidentiality Data information is protected with encryption.

Verification of data integrity The legitimacy of messages and protection against data tampering is implemented with authenticated encryption and Message Integrity Code (MIC).

Authorization policies are based on the ZTA Access to resources (control station, UAV interfaces, sensors, and actuators) is never granted until a subject, asset, or workload is verified by reliable authentication and authorization (access rules) while minimizing end-to-end latency.

A. Security Controls

IEEE P1920.2 focuses on the protection of data as a primary design criterion. Implementations lie on a technology platform that is conceived and designed to operate securely and is easy to manage. The pillars of the IEEE P1920.2 security model are as follows:

- An HSM plug-in card is mandated to store and handle security information such as cryptographic keys, PIN codes, biometrics, etc., in a secure database with full audit and log traces and secure key backup. Also, the HSM performs cryptographic functions such as key management, authentication, encryption, decryption, digital signature verification, etc. However, logistics such as

HSM tracking, and disposal are out of scope for this model. Figure 4 shows a simplified schematic diagram of a UAV board with the HSM unit.

- Use of the PKI of IEEE Wireless Access in Vehicular Environments (WAVE) or ITS-G5 to manage digital certificates.
- Use of Elliptic Curve Cryptography (ECC) with block cipher Advanced Encryption Standard (AES), WARP, or stream cipher Chacha20, both in authenticated mode.
- Authenticated Key Exchange protocol that does not require continuous access to infrastructure and operates in a distributed manner.

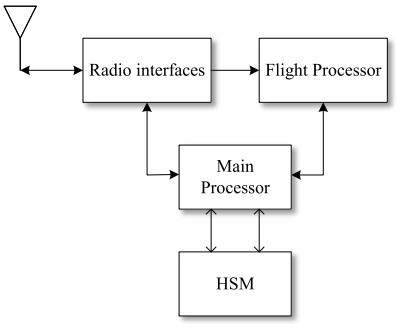

Fig. 4. Simplified schematic diagram of UAV board with HSM.

VI. UAS Security Management Framework

Security management for UAVs may involve different security management approaches and can be structured such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. As shown in Figure 5, in the V2V domain (which is the focus of IEEE P1920.2 Standardization Work Group), UAVs are equipped with various security functions such as authenticated encryption and HSMs for secure communication and computation. These low-level primitives may be augmented with embedded security monitoring (i.e., monitoring agents) and some designated sentinel UAV(s) in the environment for security management. Thus, at a higher level, operational security management can occur solely in an infrastructure-less mode (V2V mode) or can be provided via an infrastructure-extended security domain. This latter model can entail a more capable security management framework with security data collection/aggregation, security analytics, and decision-making (for security enforcement and attack countermeasures), orchestrated with a core management module. This approach may enable better situational awareness and mitigation techniques due to greater visibility and higher computational resources in this cyber-physical system. Additionally, a more holistic approach can be a federated architecture where security management systems in external domains can cooperate with the UAs domain for better security performance and protection. However, this design requires integration and coordination of systems under different jurisdictions which

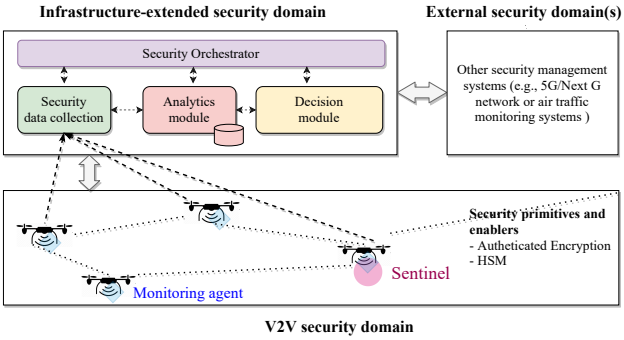

Fig. 5. Security management and different security domains for UAV networks.

may not be practical and introduce significantly higher system complexity.

VII. Zero Trust Architecture for UAS Networks

Conventional network security relies on perimeter defense concept. End users or applications frequently have broad access to network resources after they are inside the network perimeters. If such subjects are compromised, malicious actors can gain access to resources from inside or outside the network. In the IEEE P1920.2 context, a UAS forms an ad hoc network. A Zero Trust Architecture (ZTA) addresses this ad hoc network by focusing on protecting resources, not just network perimeters [10]. A ZTA-based system assumes the notion of no-implicit-trust toward assets and subjects by design. This assumption is valid regardless of physical or network locations of those entities [11]. Accordingly, a ZTA grants access to resources only aafter a subject, asset, or workload is verified via reliable authentication and authorization. The V2V radio links may be interpreted as part of a ZTA in the IEEE P1920.2 context. Then the security goal is to prevent unauthorized access to data and services while making access control enforcement as granular as possible. Since ZT is about resource access, the resource assets are the control station and UAV radio interfaces, sensors, and actuators, and not just data access in the case of UAS. The focus is on authentication, authorization (access rules), and shrinking implicit trust zones while minimizing end-to-end latency. The ZTA enables scaling while maintaining privacy and confidentiality control on the ad hoc V2V links [12].

The conceptual ZT framework model in Figure 6 shows the relationship between UAV_A and UAV_B in a V2V link and their interactions investigated in IEEE 1920.2. The ZTA authorization policy components use the control plane to communicate, while the exchange of application data uses the data plane.

The Policy Administrator (PA) is responsible for establishing or turning off the communication between a UAV access control (Agent or Gateway) and a resource (sensor, actuator, radio interface, controller) as shown in Figure 6. The terms

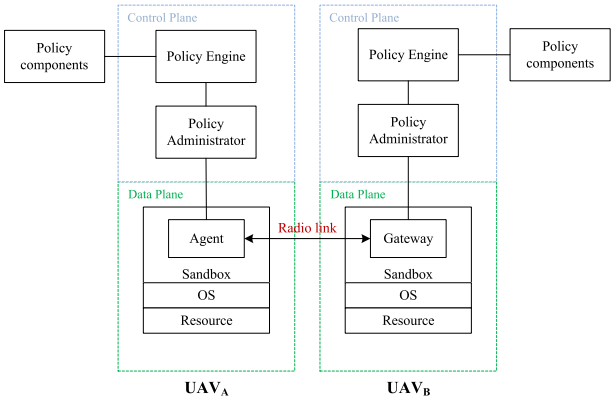

Fig. 6. Schematic representation of a V2V link with UAV$_A$ and UAV$_B$ under a ZTA.

Agent in UAV$_A$ and Gateway in UAV$_B$ follows the ZTA notation to distinguish between who requests a communication session and who accepts the request.

The secured V2V link is established between the UAV agent and the UAV gateway. Hence, the Policy Engine (PE) and PA on both sides must authenticate and authorize the communication session. If the session is granted, the PA configures the PEs to allow the session to start. If the session is denied, the PA signals to the PE to shut down the use of the UAV resource. The PE is responsible for the final decision to grant access to a resource for a particular subject. To grant, deny, or revoke access to the resource, the PE employs a trust algorithm that takes into account input from sources and an internal configuration policy. The PA executes the decision.

Figure 6 also shows the UAV resource runs on the approved, vetted applications in a sandbox. The idea is to protect an application or application instances from a compromised host or other applications running on the UAS.

The policy components provide input for policy rules used by the PE when making access decisions. These may include but are not limited to the following [11]:

Continuous diagnostics and mitigation (CDM) It gathers information about the resources' current state and applies policies and updates to configuration and software components.

Regulatory compliance It ensures the UAS remains compliant with any regulatory regime.

Threat information feed It provides information from internal or external sources for helping the policy engine to make access decisions. It may include vulnerabilities such as newly discovered flaws in software or firmware, identified malware, and reported attacks on other assets that the policy engine would want to deny access to.

Data access policies These are the attributes, rules, and policies pertaining to resource access. The rules could be embedded a priori or the policy engine may produce them dynamically. As they grant access privileges for UAS resources, these policies serve as the basis for approving access to a resource. They should be driven by the defined UAS mission role.

Public key infrastructure (PKI) It is responsible for the registration, generation, and management of digital certificates.

ID management It performs the management of user accounts, identity records, and other characteristics such as role, access attributes, and assigned assets. This component often uses other systems (such as a PKI and FAA repository) for information associated with user accounts.

Security Information and Event Management (SIEM) It gathers security-centric information for further analysis. The collected data is then used to refine/improve policies and notify about attacks against resources.

VIII. Securing Data

As we design a security protocol, we consider two baseline security system requirements:

1) Every control station (CS) and associated UAVs are equipped with a Wireless Network Interface Controller (WNIC) so that they can be configured as IP nodes in a LAN configuration.
2) The UAV controller is equipped with an embedded Linux core.

Then the designed security protocol is divided into two main parts:

1) Modern cryptographic tools at layer 3 (network layer) that provides mutually authenticated key exchange association, authenticated encryption, decryption, digital signature, and message authentication codes. Implementations may use already popular solutions like WireGuard, IPsec, or by other means. The former protocols are implemented in the Linux kernel already. Key Management embedded in the UAS for the generation and refreshment of cryptographic material to the UAS.
2) PKI for the generation, distribution, revocation, and refreshment of digital certificates to the UAS.

Accordingly, the security protocol suite supports the following functions:

- Authenticates and encrypts connections between IP nodes to provide secure communications point-to-point (unicast), one-to-many (broadcast or multicast) or mesh configuration (multicast).
- The security suite can be configured to select some traffic or all traffic to be encrypted. The V2V communication traffic can be encrypted or only authenticated depending on the configuration. Secured packets bundles a digital signature to authenticate Remote ID, which must be transmitted in the clear.
- Robust automatic reconnection after reboots or downtime.
- Modern cryptographic tools for encryption, secure association, and forward secrecy for low power devices.

After the Authenticated Key Exchange (AKE) protocol successfully authenticates UAS components, UAVs and associated

CS participating in a communication session, the key management unit generates the symmetric key used for encryption and decryption with either a block or stream cipher in IEEE P1920.2 compliant devices. The security protocol provides confidentiality and integrity of data.

As mentioned before, the security protocol uses digital certificates issued by a Certificate Authority supporting the PKI of IEEE WAVE 1609.2 or ITS-5G. Digital certificate management requires access to the PKI for the refreshment and revocation of digital certificates. However, such access to infrastructure does not have to occur every time there is a communication session. Indeed, long-term keys do not require to be refreshed in the short term. Moreover, the security protocol provides perfect forward secrecy.

However, careful monitoring of certificate revocation must be in place to avoid misbehavior or hacking activities. In case of the UAS is out of coverage from infrastructure, UAS activity may continue. Once reconnection to infrastructure is re-established, the UAS must check the status of digital certificates.

Another aspect relates to the security overhead that is within the end-to-end latency requirements for the target use cases, i.e., support of low-latency and reliable solutions. To keep user data private and secure, IEEE P1920.2 isolates security information and sensitive user data in a secure database within the HSM.

IX. Conclusion

In this paper, we have described the cyber security strategies for UAS networks in V2V mode, based on the recent work in the IEEE 1920.2 WG. The V2V communications in UAS networks require well-defined and flexible security protocols for addressing the security requirements of various use cases. For this goal, two key research questions are complexity and the level of feasible cooperation among UAVs or disparate UAS networks.

References

[1] IEEE 1920.2 WG, "IEEE P1920.2 standard for vehicle to vehicle communications for unmanned aircraft systems." https://standards.ieee.org/ieee/1920.2/7517/.

[2] D. M. Marshall, *UAS Integration into Civil Airspace*, ch. 6, pp. 133–142. John Wiley & Sons, Ltd, 2022.

[3] T. Dubot, A. Joulia, and C. L. Tallec, "Management of RPAS degraded operations: A new ATM communication architecture," in *AIAA Infotech@Aerospace (I@A) Conference*, 2013. https://arc.aiaa.org/doi/abs/10.2514/6.2013-5050.

[4] RTCA, "The Radio Technical Commission for Aeronautics (RTCA)." https://www.rtca.org/.

[5] M. K. Karyotakis, D. Panagiotakopoulos, G. Braithwaite, and A. Tsourdos, "Aspects and challenges of unmanned aircraft systems safety assurance and certification for advanced operations.," in *AIAA AVIATION 2021 FORUM*, 2021. https://arc.aiaa.org/doi/abs/10.2514/6.2021-2397.

[6] S. Verma, V. Dulchinos, R. D. Wood, A. Farrahi, R. Mogford, M. Shyr, and R. Ghatas, "Design and analysis of corridors for UAM operations," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, pp. 1–10, 2022.

[7] M. Stevens and E. Atkins, "Geofence definition and deconfliction for UAS traffic management," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2020.

[8] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," *IEEE Access*, vol. 10, pp. 112858–112897, 2022.

[9] M. Riahi Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Computers & Security*, vol. 85, pp. 386–401, 2019.

[10] A. Kerman, O. Borchert, S. Rose, E. Division, and A. Tan, *Project Description: Implementing A Zero Trust Architecture*. The National Cybersecurity Center of Excellence (NCCoE), 2020. https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf.

[11] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," tech. rep., National Institute of Standards and Technology, 2020.

[12] H. Sateesh and P. Zavarsky, "State-of-the-art VANET trust models: Challenges and recommendations," in *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0757–0764, 2020.