IEEE SA
STANDARDS
ASSOCIATION

IEEE SA
WHITE PAPER

IEEE P1920.2 WORKING GROUP

# SECURITY FOR VEHICLE-TO-VEHICLE COMMUNICATIONS FOR UNMANNED AIRCRAFT SYSTEMS

Authored by

Marco Hernandez
*Center for Wireless Communications, Oulu University, Finland*
*Yokosuka Research Park International Alliance Institute, Japan*
*National Institute of Information and Communications Technology, Japan*

Gürkan Gür
*Institute of Applied Information Technology (InIT)*
*Zurich University of Applied Sciences (ZHAW), Winterthur, Switzerland*

Shrikant Tangade
*Department of Computer Science and Engineering*
*School of Engineering and Technology, CHRIST University, Bengaluru, India*

Kamesh Namuduri
*Autonomous Systems Laboratory, University of North Texas, Denton, Texas, USA*

IEEE

## Contributors

Gerhard Schauble

*CEO, North American Aerospace, USA*

Ivan Petrunin

*Centre for Autonomous and Cyber-Physical Systems, Cranfield University, United Kingdom*

Saba Al-Rubaye

*Centre for Autonomous and Cyber-Physical Systems, Cranfield University, United Kingdom*

Ashwin Ashok

*Department of Computer Science and Affiliate in Neuroscience, Georgia State University, USA*

R. Venkatesha Prasad

*Faculty of Electrical Engineering, Mathematics, and Computer Science, TU Delft, The Netherlands*

Gary S. Griffith

*Information Technology and Data Analytics*
*The Boeing Company, USA*

Sven Bilén

*The Pennsylvania State University, USA*

## TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

*The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA*

*PDF: STDVA26059 978-1-5044-9576-9*

*IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.*

*Find IEEE standards and standards-related product listings at: http://standards.ieee.org.*

## NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA DOCUMENTS

This IEEE Standards Association ("IEEE SA") publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable and reviewed by members of the activity that produced this Work. IEEE and the IEEE P1920.2 expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE, and the IEEE P1920.2 disclaim any conditions relating to results; and workmanlike effort. This document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE P1920.2 members who have created this Work believe that the information and guidance given in it serve as an enhancement to users, all persons must rely upon their skill and judgment when making use of it. IN NO EVENT SHALL IEEE-SA OR ICAP MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, the information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holder to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all this Work may require the use of the f subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE concerning the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents. Users are expressly advised that the determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the IEEE P1920.2 members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

# TABLE OF CONTENTS

# SECURITY FOR VEHICLE-TO-VEHICLE COMMUNICATIONS FOR UNMANNED AIRCRAFT SYSTEMS

## ABSTRACT

The rapid growth of unmanned aerial vehicle (UAV) 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 unmanned aircraft systems (UAS).

The security aspects of V2V communications in UAS addressed by IEEE P1920.2 are delineated in this paper. Those include the architecture of communication interfaces, authentication of V2V parties, cryptographic key management, and zero trust architecture.

Data confidentiality and data integrity with state-of-the-art cryptographic primitives for low-power consumption implementations are comprised by data protection. In particular, UAVs' Remote ID (in cleartext) must be broadcast to comply with regulations. Hence, protection of Remote ID to avoid spoofing is done by authenticating a digital signature of such Remote ID.

Public key infrastructure (PKI) is relied upon by the trust model, but with support for use cases when UAVs are out of coverage from infrastructure.

Potential cyberattacks and their countermeasures in such systems enabling them to address vulnerabilities quickly or prevent them entirely are described in this paper.

The cybersecurity protocols addressed by IEEE P1920.2 are intended to meet the needs of:

- Regulatory requirements, including the FAA's Remote ID
- Other industry standards organizations, such as ASTM and RTCA working on the ACAS Xu solution for UAVs
- Aerospace original equipment manufacturers (OEMs) building UAVs
- Operators of UAVs

# 1. INTRODUCTION

IEEE P1920.2 defines the specification for the communication primitives of vehicle-to-vehicle (V2V) links of unmanned aerial systems (UAS).

It is assumed that UAS consist of a command and control (C2) unit and at least one unmanned aerial vehicle (UAV) associated with the C2 unit.

The information exchanged between these entities 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), beyond visual line of sight (BVLOS) but still with an active radio link, and beyond radio line of sight (BRLOS) in case of active relay.

BVLOS refers to the scenario where the UAV is not in VLOS from the control station (CS), but there is a direct radio link from the CS to the UAV. BRLOS refers to the scenario in which the UAV is not in VLOS and without a direct radio link from the CS, suggesting an intermediary relay radio link as depicted in FIGURE 1. BRLOS situations are present in hilly terrains or human developments in urban areas blocking radio waves.

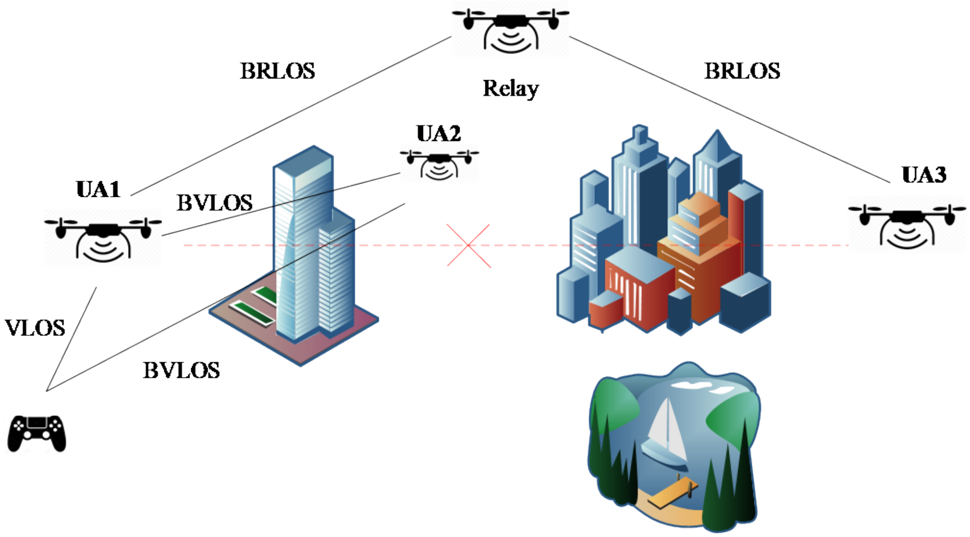

**FIGURE 1 V2V operational environment**

## 1.1. CYBERSECURITY IN UAS

### 1.1.1. GENERAL

Autonomous vehicle technology has already achieved a high degree of development. Commercial and public applications of UAS will make UAVs a part of our daily life. However, one of the biggest concerns to widespread usage of UAS is public safety and safe integration into the national airspace.

Applications involving UAVs are expected to work in urban, semi-urban, and near air traffic areas. Hence, UAS must be developed with protections against cyberattacks and faulty onboard hardware.

We present known potential cyberattacks, threats, and vulnerabilities for the operations of UAS. We propose design guidelines and mitigation strategies as countermeasures against such threats and attacks.

### 1.1.2. THREAT MODEL

Cyberattacks on UAS communications links as part of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), command and control (C2), and Global Positioning System (GPS) signals may be perceived as non-trivial, as commercial aircraft communication links do not incorporate conventional security protocols.

However, as UAS becomes more ubiquitous and networked with a wide range of applications, which will very likely incorporate access to infrastructure, integrating security provisions is of paramount importance. Indeed, by consolidating UAVs with cloud services via the cellular network or Wi-Fi, the possibility of cyberattacks increases with every unsecured communication link.

Moreover, a malicious hacker may do significant damage by taking control of a UAV by compromising the C2 communication link and GPS link to alter the flight path and provoke an accident.

IEEE P1920.2 considers attacks against the proposed protocols and data packets. We do not consider physical attacks like tampering with vehicle hardware. However, we assume that a hardware security module (HSM) in a UAV is storing cryptographic information and performing cryptographic functions.

### 1.1.3. SECURITY AND TRUST MODEL IN IEEE P1920.2

Except for physical threats such as jamming, the threats mentioned previously can be prevented by the proposed security protocol, such as:

- 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 zero trust architecture (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 reducing end-to-end latency.

Devices compliant with IEEE P1920.2 are protected against spoofing attacks of the UAS identities. Spoofing is a broad term for the type of behavior that involves a malicious party masquerading as a trusted user or device to commit malicious acts. Also, assurance that the sender of information provides proof of delivery and conversely for the recipient. Hence, neither can later deny having processed the information (non-repudiation).

IEEE P1920.2 protects the transport of data and C2 messages for V2V configurations in a decentralized manner. Also, the management of security policies for authentication, authorization, and digital certificate control is based on IEEE Std 1609.2™ [2] public key infrastructure (PKI) or ITS-G5 for Europe.

Key management enables the creation, distribution, refreshment, storage, and destruction of cryptographic keys, and in situations when a UAS is found misbehaving, there must be a mechanism for revocation of its digital certificate to prevent potential hacking or damage based on IEEE Std 1609.2 PKI or ITS-G5 policies.

Hence, V2V communication links require access to the PKI of IEEE Std 1609.2 or ITS-G5 via a connectivity network from time to time for the management of digital certificates. However, the specification of such a connectivity network is out of scope for this work.

In V2V use cases, IEEE P1920.2 supports the secure transport of data for unicast, multicast (one-to-many), and broadcast sessions with the assurance of integrity protection, with a maximum throughput of 1 Mbps, maximum latency of 1 msec, at a LOS distance up to 500 m, flying at relative speeds up to 50 km/h.

### 1.1.4. IEEE 1920.2 REFERENCE MODEL

FIGURE 2 shows the IEEE 1920.2 reference model. It illustrates the communication interfaces associated with a UAS for the different scenarios and use cases in the scope of the standard and consequently the security model.

The solid arrow lines denote the V2V communication links, unmanned aircraft link 1 (UAL1), and UAL2 as defined by IEEE 1920.2. The dotted lines show the communication interfaces of the control station (CS) for illustration only, that is, these C2 communication links are out of scope.

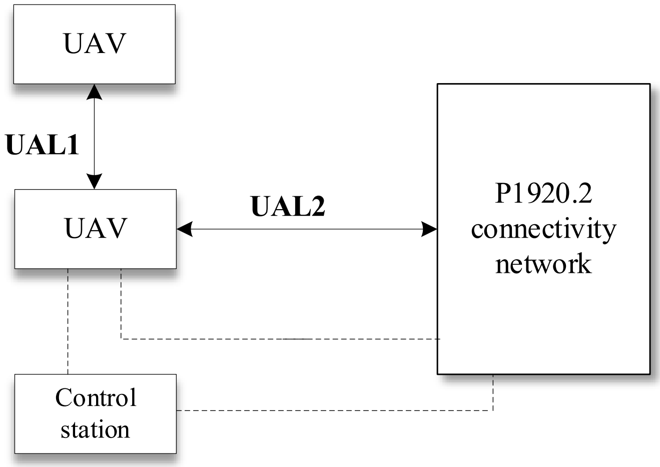

**FIGURE 2 Architecture of communication interfaces**

IEEE 1920.2 communication interfaces operate as follows:

- UAL1 interfaces UAV to the UAV communication link.

- UAL2 interfaces UAV to the connectivity network to support PKI connectivity. Such connectivity is only required for digital certificate management and so it can be offline during normal operation, and UAV may request to be online depending on the security policies, for example, when an anomaly is detected.

Such interfaces define the security provisions for confidentiality and integrity of data in transit, authentication of entities, and authorization policies.

In scenarios where the UAVs are out of coverage from the connectivity network, the security protocols perform the cryptographic functions with the credentials stored in the HSM in a UAV, pending reconnection to the connectivity network to access the PKI for management.

At any given time, a UAV may be controlled mutually exclusively by the control station (CS) directly or relay assisted, or by a detect-and-avoid mechanism, or an UAS traffic management (UTM) system. Semantics for a detect-and-avoid protocol are out of scope. UTM control protocol is an important building block, but nevertheless it is out of scope since we focus on UALs.

# 2. STATE-OF-THE-ART SECURITY

## 2.1. GENERAL

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, personal identification number (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.
- Use of the PKI of IEEE Wireless Access in Vehicular Environments (WAVE) or ITS-G5 alternative 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 (AKE) protocol that does not require continuous access to infrastructure and operates in a distributed manner.

FIGURE 3 shows a simplified schematic diagram of a UAV board with the HSM unit.

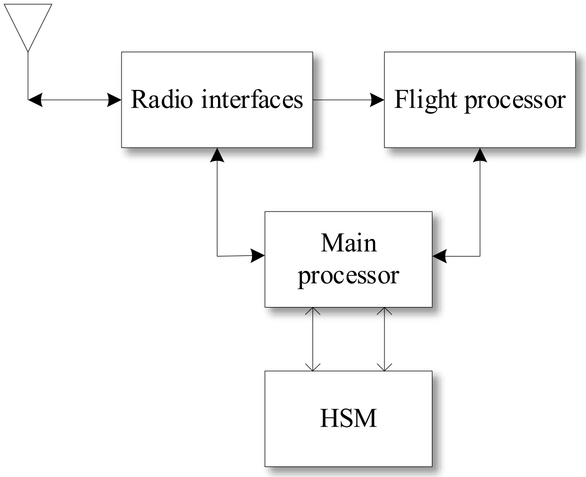

**FIGURE 3 Simplified schematic diagram of UAV board with HSM**

## 2.2. 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 [3]. As shown in FIGURE 4, in the V2V domain (which is the focus of IEEE P1920.2 Standardization Working 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.

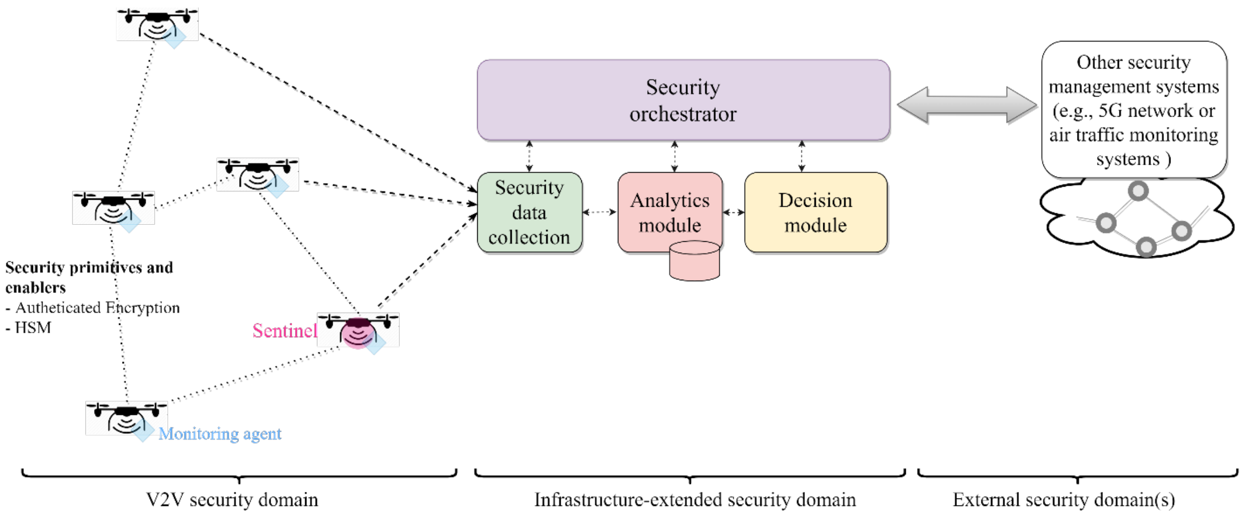
Security orchestrator
Other security management systems (e.g., 5G network or air traffic monitoring systems )
Security data collection
Analytics module
Decision module
Security primitives and enablers
- Autheticated Encryption
- HSM
Sentinel
Monitoring agent
V2V security domain
Infrastructure-extended security domain
External security domain(s)

**FIGURE 4 Security management and different security domains for UAV networks**

Additionally, a more holistic approach can be a federated architecture where security management systems in external domains can cooperate with the UAV domain for better security performance and protection. However, this design requires integration and coordination of systems under different jurisdictions, which may not be practical and introduce significantly higher system complexity.

# 3. ZERO TRUST ARCHITECTURE

Conventional network security relies on the 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, UAS form an ad hoc network.

A zero trust architecture (ZTA) addresses this ad hoc network by focusing on protecting resources, not just network perimeters [4]. A ZTA-based system assumes the notion of no-implicit-trust toward assets and subjects by design [5]. Accordingly, a ZTA grants access to resources only after 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. 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, 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.

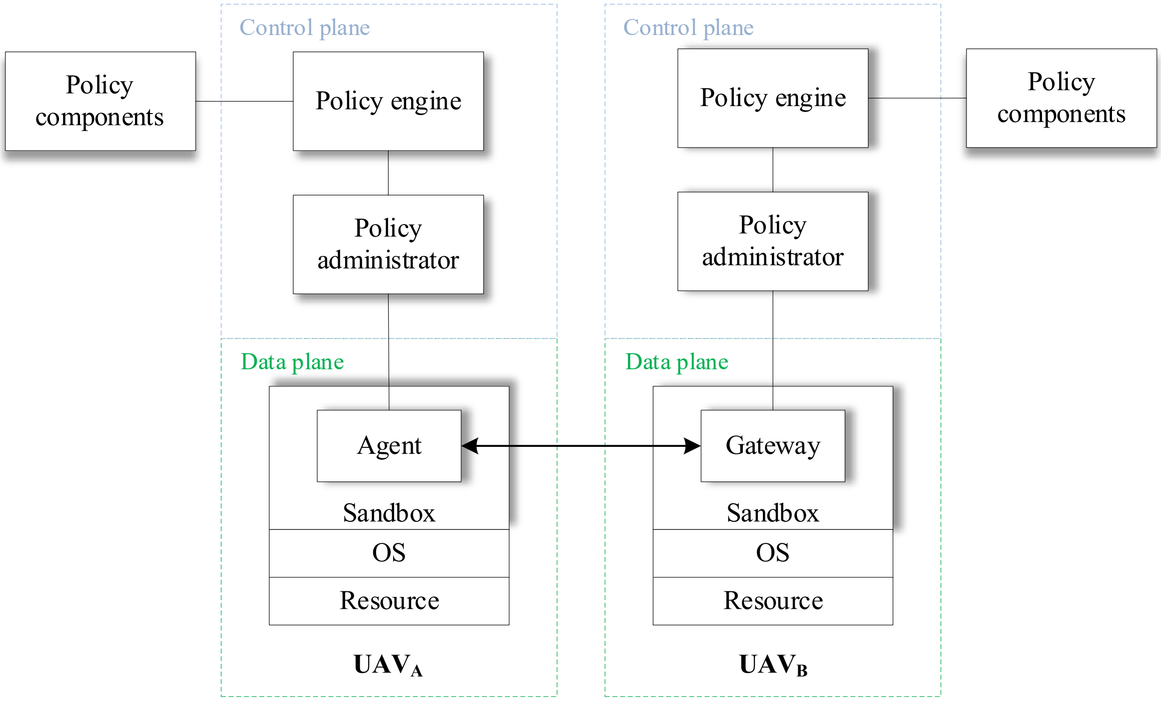

**FIGURE 5** **UAS under a ZTA**

The conceptual ZT framework model in FIGURE 5 shows the relationship between the UAS components and their interactions. 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 the UAS and a resource (in FIGURE 5 between the UAS and the UAV agent and between another UAS and the UAV gateway).

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 ultimate decision to grant access to a resource for a given subject. The PE uses an internal configuration policy and input from sources for a trust algorithm to grant, deny, or revoke access to the resource. The PA executes the decision.

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:

- *Continuous diagnostics and mitigation (CDM)* gathers information about the resources' current state and applies policies and updates to configuration and software components.
- *Regulatory compliance* ensures the UAS remains compliant with any regulatory regime.
- *Threat information feed* provides information from internal or external sources that help the policy engine make access decisions. It may include vulnerabilities, such as newly discovered flaws in software or firmware, identified malware, and reported attacks to other assets to which the policy engine will want to deny access.
- *Data access policies* are the attributes, rules, and policies about access to resources. The rules could be embedded or dynamically generated by the policy engine. These policies are the starting point for authorizing access to a resource as they provide access privileges for UAS resources. These policies should be based on the defined UAS mission role.
- *Public key infrastructure (PKI)* is responsible for the registration, generation, and management of digital certificates.
- *ID management* performs the management of user accounts, identity records, and other characteristics such as role, access attributes, and assigned assets. This system often utilizes other

systems [such as a PKI, and the Federal Aviation Administration (FAA) repository] for information associated with user accounts.

- *Security information and event management (SIEM)* collects security-centric information for later analysis. These data are used to refine policies and warn of attacks against resources.

FIGURE 4 shows the UAV resource running on the approved, vetted applications in a sandbox. The idea is to protect the application or instances of applications from a compromised host or other applications running on the UAS.

# 4. SECURING DATA

After the authenticated key exchange (AKE) protocol successfully authenticates UAS components, UAVs, and associated CS participating in a communication session, the distributed key management generates the symmetric key used for encryption and decryption with either a block or stream cipher in the IEEE P1920.2. The security protocol provides confidentiality and integrity of data. The security mechanisms are specified in the presentation and application layers of the open system interconnection (OSI) model.

As mentioned, 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. When the UAS is out of infrastructure coverage, UAS activity may continue. Once reconnection to infrastructure is re-established, the UAS must check the status of digital certificates.

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

# 5. THREAT MODEL

## 5.1. GENERAL

IEEE P1920.2 considers two types of cyberattacks: 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. Eavesdropping is a typical example. An active attack attempts to alter the system's resources or affect its operations.

## 5.2. PASSIVE ATTACKS

Passive attacks are as follows:

1. **Eavesdropping:** An attacker acquires data by interception of data traffic. If data are encrypted, an attempt to crack the encryption may be performed in real time, or the encrypted data are stored for a later attempt to decrypt it.
2. **Traffic analysis:** An attacker may be able to infer information about data transactions based on metadata of participants such as duration of transactions, timing, and other management and control data that are difficult to disguise or must be transmitted in the clear by regulations, as part of a wireless communication transaction. This type of attack attempts to infer the communication network and participants by observing their metadata exchange. It may be done as part of law enforcement surveillance or by a hacker attempting an attack.

## 5.3. ACTIVE ATTACKS

Active attacks are as follows:

1. **Impersonation:** An attacker impersonates an authorized entity to gain access to information resources. A typical case is the man-in-the-middle attack. Successful impersonation can compromise all aspects of security.

2. **Replay:** An attacker can retransmit a previous valid message to provoke a reaction. This reaction either allows the attacker to force the system into a vulnerable state or is part of a spoofing attack by message substitution.

3. **Message modification:** Modification of transmitted messages by delaying, reordering, inserting, or deleting messages or part of the information of such messages. It may also be part of a man-in-the-middle attack.

4. **Denial-of-service (DoS):** DoS occurs when an attacker compromises the availability of a system. The most common types of DoS attacks aim to disable one end of a communication session by jamming the communication channel or sending spurious signals to the target. Hence, the DoS attack deprives legitimate users of communication resources, interrupting or blocking system services to make them inaccessible. In the case of UAS, a DoS attack may occur by sending high-power wireless signals to jam any communication link. Also, a DoS attack may occur by flooding the system by continuously sending known commands or control signals to consume any available bandwidth and consequently disrupt system services.

## 5.4. UAS VULNERABILITIES

UAS vulnerabilities stem from various factors [6]:

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

Cyber threats include the following:

1. Spoofing civil GPS and Remote ID signals since those are 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 attacks target 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 to disrupt system services. Also, DoS may occur by jamming communication links.

4. Passive attacks eavesdrop C2, data communications, or telemetry.

5. Active attacks intercept and alter C2 signals, information data, GPS signals, Remote ID, and false identity information.

6. Documented cases of cyberattacks on UAS include a combination of jamming GPS signals and C2 signals to the UAV, followed by a GPS spoofing attack that fed the UAV with false GPS data to make it land in hostile territory or crash it. A variation of this attack consists of feeding the UAV with spurious C2 messages with the same malicious intent to make it land in hostile territory or crash it.

7. Consequently, feeding false detect-and-avoid messages to the UAS is a viable attack, as well as spoofing Remote ID.

8. The FAA requires Remote ID and Automatic Dependent Surveillance-Broadcast (ADS-B) messages (if applicable) to be transmitted in the clear (unsecured) to make them available to personal devices, such as Remote ID and ADS-B receivers. Such regulatory constraints make conventional encryption-based methods impractical. Therefore, a key challenge is how to develop and integrate efficient countermeasure methods against various attacks while considering the existing infrastructure and protocols [6].

9. The operation and navigation of UAS rely heavily on GPS. This dependency makes UAS navigation very difficult when GPS signals are not available.

   A UAS operating with a lost or jammed GPS signal cannot complete its mission. It endangers the safety of nearby people as well as its operating airspace. There are proposals for autonomous UAS navigation. However, these methods require intense signal processing.

   Due to the limited battery power on many small- or medium-sized UAV models, more efficient techniques are required to enable the UAS to navigate safely when GPS signals are not available.

10. Another security risk is related to the impact of cyberattacks on other subsystems such as sensors, light detection and ranging (LiDAR) systems, cameras, central processing units (CPUs), 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 (such as a cellular network or Wi-Fi access point) or provoke an accident.

Public safety is of paramount importance and, consequently, the implementation of security mechanisms in IEEE P1920.2 to protect UAS from cyberattacks.

Securing UAS is more challenging than other communication or computer networks because of the disparity in subsystems, network mobility, and diversity of data flows in C2, DAA, and data (video, audio, or image).

Current UAS supports weak security protections or nothing at all. Therefore, UAS can suffer from cyberattacks such as unauthorized connections, illegal access, malicious intent to sabotage the operation of the UAS network, or being a point of attack on infrastructure.

# 6. OPERATIONAL SECURITY

## 6.1. GENERAL

Except for physical threats such as jamming, the threats listed previously are prevented by the security protocol, such as:

1. Mutual entity authentication: Data origin authentication for sender and receiver.

2. 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.

3. Confidentiality: Data information is protected with strong encryption.

4. Perfect forward secrecy and future secrecy: The effect of a compromised key is mitigated by refreshing keys in such a way that past messages (from the instant a key was compromised) and future messages (from the instant a compromised key was refreshed) cannot be decrypted.

5. Verification of data integrity: The legitimacy of messages and protection against data tampering is implemented with authenticated encryption and message integrity code (MIC).

6. DoS protection: MAC packet filtering supports protection against DoS attacks. When authentication of packets fails, those are discarded by the link layer immediately. However, if the attacker has legitimate cryptographic credentials and the certificate has not yet been revoked, other mechanisms of DoS control are required. Those are out of the scope of the paper. Also, protection against channel jamming is out of scope.

7. Anonymity: The security protocol runs in the network layer. Hence, user information is encrypted. It offers support for privacy protection against unauthorized observers.

8. Distributed control: The security protocol is self-contained in the network layer. It is suitable for securing V2V applications when UAVs are out of coverage of infrastructure.

## 6.2. VULNERABILITY MANAGEMENT

A UAS network is a notarized system with hardware components that are also vulnerable to potential exploits due to software and hardware glitches and bugs. Therefore, during the lifecycle of these cyberphysical devices, a security management framework should detect such vulnerabilities and properly fix them with patches and software updates.

## 6.3. MONITORING

UAS security framework can monitor using monitoring agents (invasive) or traffic and physical monitoring (observational). In the first option, some monitoring agents can be deployed in UAS, which will allow data collection and measurements for security management. These modules can also be more capable and do some computation locally in an edge computing approach. In this case, a key issue is the acceptance of such an agent by different parties. Additionally, application programming interfaces (APIs) and information elements must be standardized for compatibility.

For the later approach, some sniffers and packet inspection modules can be deployed and actively monitor network traffic for suspicious and anomalous behavior. Additionally, these can be augmented with geolocation systems or physical monitoring, such as cameras and radars for location monitoring.

This monitoring capability is also instrumental for public safety agencies that are supposed to monitor UAS activity, especially in sensitive zones. Therefore, it may even be mandatory to have that based on regulations.

## 6.4. INCIDENT MANAGEMENT

As security incidents occur, they are supposed to be managed to mitigate their impact on operational systems. For UAS communications, active countermeasures may be necessary for security incidents and provide resilience as part of a pervasive UAS security framework. This function is very challenging due to the ad hoc and fragmented nature of vehicle-to-vehicle communications in UAV networks. Security management systems should be able to process security data, identify security incidents, and act based on security analytics (e.g., anomaly detection).

The counteractions may be grouped into cyber and physical counteractions. The former may involve actions such as the deployment of traffic filters, switching to more robust security primitives, as well as more severe measures such as disconnecting the UAS, revoking access, and traffic isolation for the protection of sensitive data exchange. Physical counteractions refer to physical interventions to UAS, for instance, to physically get them out of operation.

# 7. CONCLUSIONS

The protection of UAS radio links is a primary design consideration for products and operations based on IEEE 1920.2. It enables one to address vulnerabilities quickly or prevent them entirely.

The investment in cybersecurity frees implementers to focus on business and innovation.

# 8. REFERENCES

The following sources either have been referenced within this paper or may be useful for additional reading:

[ 1 ] ETSI TS 102 940 V1.3.1, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, April 2018.

[ 2 ] IEEE Std 1609.2™-2016, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages.

[ 3 ] NIST, Cybersecurity Framework v1.1. https://www.nist.gov/cyberframework.

[ 4 ] 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

[ 5 ] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture,” tech. rep., National Institute of Standards and Technology, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[ 6 ] 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.

# RAISING THE WORLD’S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571