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

Documents
Document Sharing Hub

Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

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

Documents
Document Sharing Hub

Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

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

Copyright © 2023 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 28 March 2023. Printed in the United States of America.

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

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

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

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the publisher's prior written permission.

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

Copyright © 2023 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

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.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

TABLE OF CONTENTS

ABSTRACT 6

1. INTRODUCTION 7

1.1. CYBERSECURITY IN UAS 8
1.1.1. GENERAL 8
1.1.2. THREAT MODEL 8
1.1.3. SECURITY AND TRUST MODEL IN IEEE P1920.2 9
1.1.4. IEEE 1920.2 REFERENCE MODEL 10

2. STATE-OF-THE-ART SECURITY 11

2.1. GENERAL 11

2.2. SECURITY MANAGEMENT FRAMEWORK 12

3. ZERO TRUST ARCHITECTURE 13

4. SECURING DATA 16

5. THREAT MODEL 17

5.1. GENERAL 17
5.2. PASSIVE ATTACKS 17
5.3. ACTIVE ATTACKS 17
5.4. UAS VULNERABILITIES 18

6. OPERATIONAL SECURITY 20

6.1. GENERAL 21
6.2. VULNERABILITY MANAGEMENT 21
6.3. MONITORING 21
6.4. INCIDENT MANAGEMENT 22

7. CONCLUSIONS 22

8. REFERENCES 23

Documents
Document Sharing Hub

Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

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

Copyright © 2023 IEEE. All rights reserved.

AVA Documents Document Sharing Hub

Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

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.

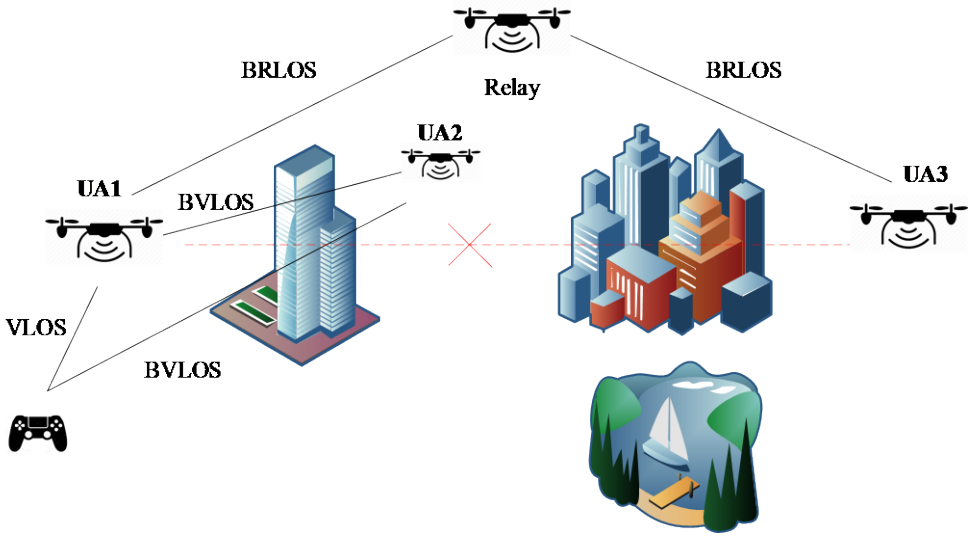


FIGURE 1 V2V operational environment

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

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.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Security For Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems