REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
17-01-2023	Final Report	1-Nov-2017 - 31-Oct-2018

4. TITLE AND SUBTITLE
Final Report: Secure On-Demand Services From the Internet of Mobile Things (IoMoT)

5a. CONTRACT NUMBER
W911NF-18-1-0012

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Universidade De Sao Paulo
Ciências de Computação
Universidade de São Paulo

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
71574-NC.19

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kalinka Regina Castelo Branco
UU	UU	UU	UU		19b. TELEPHONE NUMBER +55-163-3738

RPPR Final Report
as of 27-Jan-2023

Agency Code: 21XD

Proposal Number: 71574NC **Agreement Number: W911NF-18-1-0012**
INVESTIGATOR(S):

Name: Ph.D Kalinka Regina Lucas Jaquie Castelo Branco
Email: kalinka@icmc.usp.br
Phone Number: +551633738623
Principal: Y

Organization: **Universidade De Sao Paulo**
Address: Ciências de Computação, São Carlos, 13.566590
Country: BRA
DUNS Number: 900060369 EIN:
Report Date: 31-Jan-2019 Date Received: 17-Jan-2023
Final Report for Period Beginning 01-Nov-2017 and Ending 31-Oct-2018
Title: Secure On-Demand Services From the Internet of Mobile Things (IoMoT)
Begin Performance Period: 01-Nov-2017 **End Performance Period:** 31-Oct-2018
Report Term: 0-Other
Submitted By: Ph.D Kalinka Regina Castelo Branco Email: kalinka@icmc.usp.br
Phone: (+55) 163-3738623
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 4 **STEM Participants:** 2

Major Goals: The major goals In this project we proposed to start in the first level of attacks, focusing on a single UAV. Mainly two types of attacks will be studies: GPS Spoofing that has become a frequent attack that helps attackers to hijack drone. We already have in our labs solutions to generate fake GPS signals based on GNU radio and software defined radio boards.

Another issue that is strongly related to the first one is a man-in-the-middle attacks that will be investigated in the project. These two attacks are really related with the chosen
scenarios.

An original solution based on pairs of intricately linked supervisors located in the device and in the Datacenter, to detect and identify the different kinds and levels of attacks. So, a strategy to address cybersecurity vulnerability, once identified, must understand the nature of the vulnerability and how to mitigate it. The resource limitation will be considered in the implementation techniques to be developed. Actions will be associated with the Supervisor.

We also develop strategies for security countermeasure using cognitive radio.

Accomplishments: 1) major activities
Communication security is one of the most critical issues related to UAVs. Multi-UAV systems extends the attack surface, and node mobility also impacts security with frequent network topology changes and link inconsistency. UAS design and development must take security issues into account so the system can answer autonomously and dynamically to attacks or failures, whether accidental or intentional. Conventional security mechanisms are not efficient for real-time transmission required by UAVs, making distributed solutions that do not depend on the GCS and do not compromise UAV resources or network performance necessary

All UAS components present vulnerabilities that can be exploited and result in a security breach or a system control loss. UAVs rely on different systems (navigation, collision avoidance, sensing) to operate. If any of them is compromised or tampered with, the UAV can be lost and accept malicious commands. Also, UAV systems that depend on external plain signals such as GPS navigation or collision avoidance can receive falsified data and alter the way the aircraft operates. The GCS must be protected against software threats such as malware and hardware tampering. Communication links in a UAS can be employed in many ways, and each one has its own set of vulnerabilities.

GPS Jamming or Spoofing

UAV navigation depends heavily on Global Navigation Satellite System (GNSS), being the Global Positioning System (GPS) the most common option. Without this signal, a UAV may be susceptible to Denial of Service (DoS) and/or errors in measurements that can lead the vehicle to crash or diverted from its course. GPS signals can be either jammed --- when a stronger signal jams the channel and make the receiver unable to distinguish the original GPS signal --- or easily spoofed--- when a faked signal injects false positioning information to the UAV. The lack of authentication in civil GPS signals makes it easy for its falsification with low-cost equipment and the GPS receiver unable to discern if the received signal is authentic or not.

- Countermeasures: Authenticated GPS signals could prevent GPS spoofing. Such strategy, however, would require changes in the entire satellite system. Surveillance of GPS signal for sudden changes in signal strength and traveling time can give indications of signal spoofing. In order to counter GPS jamming, alternative navigation methods such as vision and/or inertial navigation systems can be employed in the absence of GPS signals.

Signal Jamming or Spoofing

It is expected UAVs will emit broadcasts with its own position and velocity to be used by other aircraft in their collision avoidance system. Like GPS, this broadcast would be open and therefore easily jammed or spoofed, which could lead to UAV collisions or insertion into unfriendly territory. Spoofing UAV telemetry and video feeds can influence operator commands and compromise the system operation. Jamming GCS control signals can induce the UAV into an emergency protocol and impede mission realization. With GCS control signal spoofing, the adversary can take control of the aircraft.

- Countermeasures: UAV signal authenticity verification is necessary to ensure reliable information. In the case of jammed GCS control signals, UAV response needs to be carefully planned so it will not act unpredictably if others signals, such as GPS, are also jammed. In the case of a fixed GCS location-based authentication can be used to mitigate spoofing.

Information Injection

Without proper identification and authentication schemes, a malicious user can pose as a trusted UAV or UAV module and inject the system with falsified information, destabilizing UAVs and compromising UAS operation.

- Countermeasures: Authentication of all UAVs modules and of the UAVs within a FANET is necessary to ensure only reliable information is being received. Also, comparing the expected behavior/data from actual provided information from modules can identify discrepancies and identify possible falsified data.

Malicious Hardware or Software

Both GCS and UAV systems are exposed to hardware and software trojan. GCS can be infected by the actions of an unsuspecting operator or through a connection to an external system or the Internet itself. Hardware trojan can be inserted in chips during fabrication and disable security mechanisms or provide a back door for adversaries.

- Countermeasures: Intrusion detection systems, antivirus software, firewalls, and other policies can mitigate the threat of software trojan and malware. The use of reliable hardware suppliers as well as side-channel analysis minimize the risk of hardware trojan.

Unauthorized Disclosure of Communication

Exchanged information between UAVs or between the UAV and the infrastructure needs to be protected against unauthorized disclosure when intercepted.

- Countermeasures: Employing cryptography can ensure data confidentiality and integrity. Elliptic curve cryptography solutions can be used to provide a good security level with less resource consumption than other public-key solutions. However, implementing a Certification Authority functionality in an ad-hoc network is challenging and may fail depending on the employed approach.

Denial of Service (DoS)

Both the infrastructure and UAVs can be at risk of DoS. In a centralized communication UAS, a DoS in GCS will leave all UAVs in the system without receiving any control commands. In a decentralized UAS, compromising the GCS availability can impede UAVs to send pertinent mission information to a remote operator or system. Flooding UAVs with random commands can force them into an unexpected state and consequently compromise UAS operation.

- Countermeasures: UAVs and GCS need to implement mechanisms that made them resistant to DoS. Implementing contingency policies for DoS situations can prevent the system from achieving an unexpected state.

2) specific objectives

The objectives of the project were achieved.

3) significant results, including major findings, developments, or conclusions (both positive and negative)

As results, this project create the ground for the development of specific techniques for securing the future IoMoT considering mobility, criticality and scalability. In this first year the results and contributions can be summarized as:

- A comparison of available features of unmanned aircraft systems, Internet of Things, and the new Internet of Flying Things.
- A systematic approach that can put together all kinds of attacks and vulnerabilities once the information is spread in the literature - UASs, Internet of Things, Cloud Computing and Mobility Things security.
- A systematic and context-aware model-based approach to support dependability analysis of unmanned aerial vehicles. The approach was built upon compositional dependability analysis techniques.
- Security policies, mechanism and strategies to overcome the security problem - the use of Cognitive Radio and Cloud-SPHERE.
- Energy consumption study, to allow the UAV to flight in the context of IoMoT and can also improve the system's safety and point to potential problems or attacks.

4) key outcomes or other achievements. Include a discussion of stated goals not met. As the project progresses, the emphasis in reporting in this section should shift from reporting activities to reporting accomplishments.

For the next steps we are planning to develop some strategies to Aerial Taxis.

Training Opportunities: Nothing to Report

Results Dissemination: We publish lots of paper in journals and conferences.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: Co-Investigator
Participant: Jean-Philippe Diguet
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

Participant Type: Co-Investigator
Participant: Rosana Vaccare Braga
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

Participant Type: Co-Investigator
Participant: Catherine Dezan
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

RPPR Final Report
as of 27-Jan-2023

Participant Type: Co-Investigator
Participant: Daniel Fermando Pigatto
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

Participant Type: Co-Investigator
Participant: Natassya Barlate Silva
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

Participant Type: Co-Investigator
Participant: Matheus Franco
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

Participant Type: Co PD/PI
Participant: Mariana Rodrigues
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

Participant Type: Undergraduate Student
Participant: Daniel Xavier
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
National Academy Member: Y

International Travel:

BRA 7 days

BRA 90 days

ARTICLES:

RPPR Final Report
as of 27-Jan-2023

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Sensors
Publication Identifier Type: DOI Publication Identifier: 10.3390/s21030830
Volume: 21 Issue: 3 First Page #: 830
Date Submitted: 1/17/23 12:00AM Date Published: 1/1/21 6:00AM
Publication Location:
Article Title: Integrating Cognitive Radio with Unmanned Aerial Vehicles: An Overview
Authors: Guilherme Marcel Dias Santana, Rogers Silva de Cristo, Kalinka Regina Lucas Jaquie Castelo Branco
Keywords: unmanned aerial vehicles; cognitive radio networks; software defined radio; network sensing; security; internet of flying things; machine learning; energy management
Abstract: Unmanned Aerial Vehicles (UAVs) demand technologies so they can not only fly autonomously, but also communicate with base stations, flight controllers, computers, devices, or even other UAVs. Still, UAVs usually operate within unlicensed spectrum bands, competing against the increasing number of mobile devices and other wireless networks. Combining UAVs with Cognitive Radio (CR) may increase their general communication performance, thus allowing them to execute missions where the conventional UAVs face limitations. CR provides a smart wireless communication which, instead of using a transmission frequency defined in the hardware, uses software transmission. CR smartly uses free transmission channels and/or chooses them according to application's requirements. Moreover, CR is considered a key enabler for deploying technologies that require high connectivity, such as Smart Cities, 5G, Internet of Things (IoT), and the Internet of Flying Things (IoFT). This paper presents an overview on t
Distribution Statement: 2-Distribution Limited to U.S. Government agencies only; report contains proprietary info
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Journal of Intelligent & Robotic Systems
Publication Identifier Type: DOI Publication Identifier: 10.1007/s10846-022-01764-4
Volume: 106 Issue: 3 First Page #: 62
Date Submitted: 1/17/23 12:00AM Date Published: 11/1/22 3:00AM
Publication Location:
Article Title: Path-following Algorithms Comparison using Software-in-the-Loop Simulations for UAVs
Authors: Daniel M. Xavier, Natassya B. F. Silva, Kalinka R. L. J. C. Branco
Keywords: Carrot-chasing · Genetic algorithm · NLGL · Path-following · PLOS · Software-in-the-Loop · Unmanned aerial vehicles · Vector field
Abstract: Unmanned Aerial Vehicles (UAVs) demand technologies so they can not only fly autonomously, but also communicate with base stations, flight controllers, computers, devices, or even other UAVs. Still, UAVs usually operate within unlicensed spectrum bands, competing against the increasing number of mobile devices and other wireless networks. Combining UAVs with Cognitive Radio (CR) may increase their general communication performance, thus allowing them to execute missions where the conventional UAVs face limitations. CR provides a smart wireless communication which, instead of using a transmission frequency defined in the hardware, uses software transmission. CR smartly uses free transmission channels and/or chooses them according to application's requirements. Moreover, CR is considered a key enabler for deploying technologies that require high connectivity, such as Smart Cities, 5G, Internet of Things (IoT), and the Internet of Flying Things (IoFT). This paper presents an overview on t
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Jan-2023

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Access
Publication Identifier Type: DOI Publication Identifier: 10.1109/ACCESS.2019.2915561
Volume: 7 Issue: First Page #: 59737
Date Submitted: 1/17/23 12:00AM Date Published:
Publication Location:
Article Title: The Broadcast Storm Problem in FANETs and the Dynamic Neighborhood-Based Algorithm as a Countermeasure
Authors: Rayner M. Pires, Alex Sandro Roschildt Pinto, Kalinka Regina Lucas Jaquie Castelo Branco
Keywords: Broadcast mitigation techniques, data dissemination protocols, FANETs, flooding, UAV communication, wireless ad hoc communication.
Abstract: Unmanned Aerial Vehicles (UAVs) demand technologies so they can not only fly autonomously, but also communicate with base stations, flight controllers, computers, devices, or even other UAVs. Still, UAVs usually operate within unlicensed spectrum bands, competing against the increasing number of mobile devices and other wireless networks. Combining UAVs with Cognitive Radio (CR) may increase their general communication performance, thus allowing them to execute missions where the conventional UAVs face limitations. CR provides a smart wireless communication which, instead of using a transmission frequency defined in the hardware, uses software transmission. CR smartly uses free transmission channels and/or chooses them according to application's requirements. Moreover, CR is considered a key enabler for deploying technologies that require high connectivity, such as Smart Cities, 5G, Internet of Things (IoT), and the Internet of Flying Things (IoFT). This paper presents an overview on t
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Journal of Intelligent & Robotic Systems
Publication Identifier Type: DOI Publication Identifier: 10.1007/s10846-019-01046-6
Volume: 97 Issue: 1 First Page #: 249
Date Submitted: 1/17/23 12:00AM Date Published: 6/1/19 3:00AM
Publication Location:
Article Title: Cloud–SPHERE: Towards Secure UAV Service Provision
Authors: Mariana Rodrigues, Kalinka Regina Lucas Jaquie Castelo Branco
Keywords: UAV · IoT · Security · Safety · Service · HAMSTER · Cloud–SPHERE
Abstract: Unmanned Aerial Vehicles (UAVs) demand technologies so they can not only fly autonomously, but also communicate with base stations, flight controllers, computers, devices, or even other UAVs. Still, UAVs usually operate within unlicensed spectrum bands, competing against the increasing number of mobile devices and other wireless networks. Combining UAVs with Cognitive Radio (CR) may increase their general communication performance, thus allowing them to execute missions where the conventional UAVs face limitations. CR provides a smart wireless communication which, instead of using a transmission frequency defined in the hardware, uses software transmission. CR smartly uses free transmission channels and/or chooses them according to application's requirements. Moreover, CR is considered a key enabler for deploying technologies that require high connectivity, such as Smart Cities, 5G, Internet of Things (IoT), and the Internet of Flying Things (IoFT). This paper presents an overview on t
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

RPPR Final Report
as of 27-Jan-2023

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)
Date Received: 31-Aug-2018 Conference Date: 25-Jun-2018 Date Published:
Conference Location: Luxembourg
Paper Title: Model-Based Dependability Analysis of Unmanned Aerial Vehicles - A Case Study
Authors: Matheus Franco, Rosana Braga, André Oliveira, Catherine Dezan, Jean-Philippe, Kalinka Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Workshop on Communications in Critical Embedded Systems
Date Received: 17-Jan-2023 Conference Date: 25-Jun-2018 Date Published:
Conference Location: Natal, Brazil
Paper Title: MARIO: A Cognitive Radio Primary User Arrivals Data Generator
Authors: Rogers Cristo, Guilherme Santana, Diana Osorio, Kalinka Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Workshop on Communications in Critical Embedded Systems
Date Received: 17-Jan-2023 Conference Date: 25-Jun-2018 Date Published:
Conference Location: Natal, Brazil
Paper Title: Navigation Phases Platform: Towards Green Computing for UAVs
Authors: Mariana Rodrigues, Daniel Pigatto, Kalinka Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Workshop on Communications in Critical Embedded Systems
Date Received: 17-Jan-2023 Conference Date: 25-Jun-2018 Date Published:
Conference Location: Natal, Brazil
Paper Title: Comparison of path-following algorithms for loiter paths of Unmanned Aerial Vehicles
Authors: Daniel Xavier, Natassya Silva, Kalinka Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: International Conference on Unmanned Aircraft Systems (ICUAS'18)
Date Received: 17-Jan-2023 Conference Date: 11-Jun-2018 Date Published:
Conference Location: Dallas, USA
Paper Title: Cognitive Radio for UAV communications: Opportunities and future challenges
Authors: Guilherme Santana, Rogers Cristo, Catherine Dezan, Jean-Philippe Diguet, Diana Osório, Kalinka Brar
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: International Conference on Unmanned Aircraft Systems (ICUAS'18)
Date Received: 17-Jan-2023 Conference Date: 11-Jun-2018 Date Published:
Conference Location: Dallas, USA
Paper Title: Cloud–SPHERE: A Security Approach for Connected Unmanned Aerial Vehicles
Authors: Mariana Rodrigues, Daniel Pigatto, Kalinka Branco
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Jan-2023

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Workshop on Communications in Critical Embedded Systems (as part of IEEE ISCC 2019)
Date Received: 17-Jan-2023 Conference Date: 30-Jun-2019 Date Published: 01-Jul-2019
Conference Location: Barcelona
Paper Title: Control validation with software-in-the-loop for a fixed-wing vertical takeoff and landing unmanned aerial vehicle with multiple flight stages
Authors: Natassya, Silva; João, Fontes; Kalinka, Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Workshop on Communications in Critical Embedded Systems (as part of IEEE ISCC 2019)
Date Received: 17-Jan-2023 Conference Date: 01-Jul-2019 Date Published: 01-Jul-2019
Conference Location: Barcelona
Paper Title: Path-following algorithms comparison using Software-in-the-Loop simulations for UAVs
Authors: Daniel, Xavier; Natassya, Silva; Kalinka, Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: UAVs at Your Service: Towards IoT Integration with HAMSTER
Date Received: 17-Jan-2023 Conference Date: 12-Jun-2019 Date Published: 15-Jun-2019
Conference Location: Atlanta
Paper Title: UAVs at Your Service: Towards IoT Integration with HAMSTER
Authors: Mariana, Rodrigues; Kalinka, Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Workshop on Communications in Critical Embedded Systems (as part of IEEE ISCC 2019)
Date Received: 17-Jan-2023 Conference Date: 01-Jul-2019 Date Published: 01-Jul-2019
Conference Location: Barcelona
Paper Title: Authentication Methods for UAV Communication
Authors: Mariana, Rodrigues; Jean, Amaro; Fernando, Osório; Kalinka, Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2020 IEEE Symposium on Computers and Communications (ISCC)
Date Received: 17-Jan-2023 Conference Date: 07-Jul-2020 Date Published:
Conference Location: Rennes, France
Paper Title: Context-Aware Operation for Unmanned Systems with HAMSTER
Authors: Mariana, Rodrigues; Daniel, Pigatto; Kalinka, Branco
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2019 16th International Symposium on Wireless Communication Systems (ISWCS)
Date Received: 17-Jan-2023 Conference Date: 27-Aug-2019 Date Published:
Conference Location: Oulu, Finland
Paper Title: Opportunities for autonomous UAV in harsh environments
Authors: Rodrigo, La Scalea; Mariana, Rodrigues; Diana, Osório; C, Lima; R, Souza; H, Alves; Kalinka, Branco
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 27-Jan-2023

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Kalinka Regina Lucas Jaquie (
Signature Date: 1/17/23 8:59PM

Final Report

Abstract

Groups of heterogeneous autonomous vehicles (aerial, ground, underwater, etc) are going to invest human environment including battlefields. Due to their characteristics, they are natural candidates to integrate the Internet of Things (IoT), a dynamic and global network infrastructure where intelligent nodes are interconnected. By including autonomous vehicles into IoT, it will be possible to compose the Internet of Mobile Things (IoMoT), which introduces new opportunities and challenges. IoMoT offers the number, so the parallelism, a hierarchical infrastructure (UAV, SWARM, Data center), redundancy, mobile and multiple view angles and cooperation possibilities. But IoMoT also raises challenges related to scalability, group control, synchronization, power consumption, limited embedded resources and limited action time so an important turnover. All these dimensions introduce manifold security issues, so in this project we will focus on security considering the global future IoMoT context. The main goal of this research is to create the ground for the development of specific techniques for securing the future IoMoT considering mobility, criticality and scalability.

1 Objectives for the entire research project, specifically noting the objectives for each grant year

A brief definition for Unmanned Vehicle (UV) is a vehicle without a person on board. Also seen as uncrewed vehicles, they can be remotely or autonomously controlled, usually applied in a wide range of environmental sensing activities, high risk areas monitoring, driving assistance, monitoring activities and much more.

Over the last years, aerial and ground vehicle systems have been receiving an increased number of electronic components, running embedded software, and connected through wireless communication channels. This strong integration between dedicated computing devices, the physical environment and networking, has become part of common Unmanned Aerial Vehicles (UAV) likely to be commonplace and accessible to everyone in the near future. Furthermore, as processing power increases and software becomes more sophisticated, these vehicles gain the ability to perform complex operations, becoming more autonomous, efficient, adaptable, safe and usable. UAVs may be deployed in environments where physical accessibility is difficult or impossible.

UAVs are classified as safety-critical, once failure events may cause injury or the loss of high-value assets, meaning that safety is one of the main concerns for developers and users. However, the combination of high mobility and wireless communications has further increased the exposure of these systems to malicious threats and to faults deriving from uncertain connectivity or communication timeliness. Non-functional requirements like security have thus become harder to fulfill, creating new challenges to such safety-critical embedded systems. There is massive research interest on this field as smart drones, cars and boats take place, get cheaper, easier to control and even more integrated to everyday situations. However, a major concern on these vehicles' acceptance and certification still relies on safety and security issues, apart from other requirements that must be met as new vehicles are developed. Our project is first based on an in-depth study of security requirements based on the state of the art attacks.

2 Results

As results, this project create the ground for the development of specific techniques for securing the future IoMoT considering mobility, criticality and scalability. In this first year the results and contributions can be summarized as:

- A comparison of available features of unmanned aircraft systems, Internet of Things, and the new Internet of Flying Things.
- A systematic approach that can put together all kinds of attacks and vulnerabilities once the information is spread in the literature - UASs, Internet of Things, Cloud Computing and Mobility Things security.
- A systematic and context-aware model-based approach to support dependability analysis of unmanned aerial vehicles. The approach was built upon compositional dependability analysis techniques.
- Security policies, mechanism and strategies to overcome the security problem - the use of Cognitive Radio and Cloud-SPHERE.
- Energy consumption study, to allow the UAV to flight in the context of IoMoT and can also improve the system's safety and point to potential problems or attacks.

2.1 Internet of Flying Things

Unmanned aircraft systems have received a lot of attention lately, especially due to their flexibility and reduced acquisition costs. However, in many regions, legislation issues have emerged that curtail their operation in critical environments. In response to well-reported instances, it seems likely that in many countries “no-fly” zones will be established around critical areas, such as airports (where accidental “drone-strikes” could pose a threat to jet planes similar to “bird-strikes”), prisons (where cases have been reported of drones being used to transport contraband goods in to prisoners), and military/confidential areas (where government is combating drones with trained eagles). Security threats from terrorist groups also pose a risk to key infrastructure. In the future, it seems likely that international consensus may arise around certain areas (e.g., commercial airports) but the picture is likely to remain fluid for some time. Meanwhile, significant research efforts are exploring the current capabilities of UAVs, and their potential for autonomous action beyond the line of sight of a dedicated operator, which is likely to fuel further debate and legislation.

The relatively recent concept of Internet of Things (IoT), which consists of a new form of connecting and sharing resources among devices, has been considered as a candidate for potential integration with unmanned aircraft. Such collaboration may provide a new degree of freedom for old applications and a completely new spectrum of applications.

We start our studies with a revision of the main characteristics of the Internet of Flying Things (IoFT) and how the term is related to unmanned aircraft systems and the Internet of Things. So we provide a comparison of available features of unmanned aircraft systems, Internet of Things, and the Internet of Flying Things (IoMot is IoFT-based).

There are understandable concerns about the threat that networked UAVs (FANET - Flying Ad hoc NETworks) could pose to privacy and safety. Legislation is likely to address the design and usage of IoFT-based systems, and to help with public confidence the largest open challenge facing the field is the development and adoption of robust standards for security and safety—of both devices and the data they carry and transmit.

Considering the many physical forms that a UAV might take, security policies and algorithms must be devised that are resource efficient, work on many different types of hardware (from data storage devices right through to different aircraft chassis) and software (across the layers of network protocols). When one extends the considerations to multi-UAV swarms, or even disparate groups connected via a WFANET (Wide FANET), policies must then take into account the greater "vulnerable surface" of an ad hoc network, and redundancy of information (encryption keys, etc.) that will arise as mobile devices become unavailable for periods of time as they move around.

Features	Internet of Things (IoT)	Unmanned aircraft systems (UAS)	Internet of Flying Things (IoFT)
Cooperation	Limited by IoT infrastructure	Limited by FANET infrastructure	Includes all the IoT and FANET infrastructure capabilities
Collaboration	Limited by IoT infrastructure	Limited by FANET infrastructure	Includes all the IoT and FANET infrastructure capabilities
Real-time operations	Limited to the network coverage	Limited to the actuation areas	Reduced limitations due to increased connectivity
Connectivity	Internet connected	Locally connected by a FANET	Highly connected—not just to the Internet, but also locally connected
Up-to-date data/ services	Available	Weakly available	Available
Internet-based information processing	Available	Weakly available	Available
Interactive decision-making	Available	Available	Available with higher flexibility
Mission-assistive multisource information providers	Available	Weakly available	Available with higher variety of sources

2.2 Security for Connected Vehicles

Based on the issues that can be solved (including some kinds of attacks), we did a deeply study in Security and privacy in UAS (Unmanned Aerial System) and in Internet of Things taking into account the mobility aspect. Once thinking in IoT, the cloud computing security was also detailed. With this we put together all kinds of attacks and vulnerabilities in the IoMoT, once we treat the device (part of the UAS), the IoT and all peculiarities existing in the IoMoT.

Once the paper was just submitted and need to be an original one, in this report we will just present the Security in UASs.

Security and Privacy are the most critical issues regarding UAVs. UAS design and development must take security issues into account so the system can answer autonomously and dynamically to attacks or failures, whether accidental or intentional. Conventional security mechanisms, however, are not efficient for real-time transmission required by UAVs. Regarding a UAS, the following security requirements apply:

- Availability -- all elements of a UAV must perform their tasks without any disruption during its operation, even if the aircraft is under attack.
- Confidentiality -- Communication between UAVs or between the UAV and the infrastructure can not leak information to unauthorized parties.
- Integrity -- In UASs, integrity can refer to information integrity or system integrity. Information integrity ensures that exchanged data in communication links, such as mission data, telemetry and GPS signals have not been altered. System integrity ensures the authenticity of software and hardware components.
- Accountability -- UASs need accountability mechanisms to ensure non-repudiation. A digital signature algorithm can bind the action to an entity, and logging procedures allow action tracking.
- Authentication and access control -- Identification and authentication of nodes are necessary for secure communication. When a node is inserted in the network, it must be identified and authenticated before communicating with other nodes within the network. Access control policies are necessary to prevent unauthorized personnel from accessing sensitive data and/or control operations.

All UAS components present vulnerabilities that can be exploited and result in a security breach or a system control loss. UAVs rely on different systems (navigation, collision avoidance, sensing) to operate. If any of them is compromised or tampered with, the UAV can be lost and accept malicious commands. Also, UAV systems that depend on external plain signals such as GPS navigation or collision avoidance can receive falsified data and alter the way the aircraft operates. The GCS must be protected against software threats such as malwares and hardware tampering. Communication links in a UAS can be employed in many ways, and each one has its own set of vulnerabilities. Next, main threats to a UAS are discussed.

2.3 Denial of Service (DoS)

Both the infrastructure and UAVs can be at risk of DoS. In a centralized communication UAS, a DoS in GCS will leave all UAVs in the system without receiving any control commands. In a decentralized UAS, compromising the GCS availability can impede UAVs to send pertinent mission information to a remote operator or system. Flooding UAVs with random commands can force them in an unexpected state and consequently compromise UAS operation.

- Countermeasures UAVs and CGS need to implement mechanisms that made them resistant to DoS. Implementing contingency policies for DoS situations can prevent the system from achieving an unexpected state.

2.4 GPS Jamming or Spoofing

UAV navigation depends on free, plain and unauthenticated GPS signals received and processed by a GPS receiver. GPS signals can be spoofed (the UAVs are fed with a fake GPS signal) and easily jammed, which can compromise UAV navigation and leading it to crash or lend in an unfriendly site. Also, GPS receiver can be compromised by malwares and compromise UAV navigation.

- Countermeasures Authenticated GPS signals could prevent GPS spoofing. Such strategy, however, would require changes in the entire satellite system. Surveillance of GPS signal for sudden changes in signal strength and travelling time can give indications of signal spoofing. In order to counter GPS jamming, alternative navigation methods such as vision and/or inertial navigation systems can be employed in the absence of GPS signals.

2.5 Information Injection

Without proper identification an authentication schemes, a malicious user can pose as a trusted UAV or UAV module and inject the system with falsified information, destabilizing UAVs and compromising UAS operation.

- Countermeasures Authentication of all UAVs modules and of the UAVs within a FANET is necessary to ensure only reliable information is being received. Also, comparing the expected behaviour/data from actual provided information from modules can identify discrepancies and identify possible falsified data.

2.6 Malicious Hardware or Software

Both GCS and UAV systems are exposed to hardware and software trojans. GCS can be infected by the actions of a unsuspecting operator or through a connection to an external system or the Internet itself. Hardware trojans can be inserted in chips during fabrication and disable security mechanisms or provide a back door for adversaries.

- Countermeasures Intrusion detection systems, antivirus software, firewalls, and other policies can mitigate the threat of software trojans and malwares. The use of reliable hardware suppliers as well as side-channel analysis minimize the risk of hardware trojans.

2.7 Signal Jamming or Spoofing

It is expected UAVs will emit a broadcast with its own position and velocity to be used by other aircraft in their collision avoidance system. Like GPS, this broadcast would be open and therefore easily jammed or spoofed, which could lead to UAV collisions or insertion into unfriendly territory. Spoofing UAV telemetry and video feeds can influence operator commands and compromise the system's operation. Jamming GCS control signals can induce the UAV into an emergency protocol and impede mission realization. With GCS control signal spoofing, the adversary can take control of the aircraft.

- Countermeasures UAV signal authenticity verification is necessary to ensure reliable information. In case of jammed GCS control signals, UAV response need to be carefully planned so it won't act unpredictably if other signals such as GPS are also jammed. In the case of a fixed GCS, location-based authentication can be used to mitigate spoofing.

2.8 Unauthorized Disclosure of Communication

Exchanged information between UAVs or between the UAV and the infrastructure needs to be protected against unauthorized disclosure when intercepted.

- Countermeasures Employing cryptography can ensure data confidentiality and integrity. Elliptic curve cryptography solutions can be used to provide good security level with fewer resource consumption than other public key solutions. However, implementing a Certification

Authority functionality in an ad-hoc network is challenging and may fail depending on the employed approach.

It is important to mention that the impact of any employed security solution in the system needs to be analyzed. Delays in transmission and processing, as well as a system overhead introduced by security measures need to be evaluated to ensure that real-time constraints are met and that UAS is operating satisfactorily.

2.9 Dependability Analysis of Unmanned Aerial Vehicle

Once facing the attacks and the vulnerabilities from all parts that compose the IoMoT we addressed the dependability problem, mapping the safety issues to determine the interdependence between safety and security. Solutions were analyzed based on the results of a fault tree/attack tree of the autonomous vehicle system.

Safety-critical systems (SCS) are computer systems in which the occurrence of failures may lead to catastrophic consequences. Unmanned Aerial vehicle (UAV) is a kind of complex safety-critical system that comprises the unmanned aircraft, its payload, the ground control station (GCS) and communication links between the UAV and GCS. The development of safety-critical systems in the UAV domain has to address guidance defined in DO-178C and SAE ARP 4754A aerospace safety standards. These standards establish that dependability properties of a given critical system should be analyzed and demonstrated at different levels of abstraction before its release for operation and achieving safety-certification. Dependability analysis can be defined as the identification, early on the design, of potential threats to system reliability, availability, integrity, and safety, their potential causes, and measures to avoid or minimizing their effects.

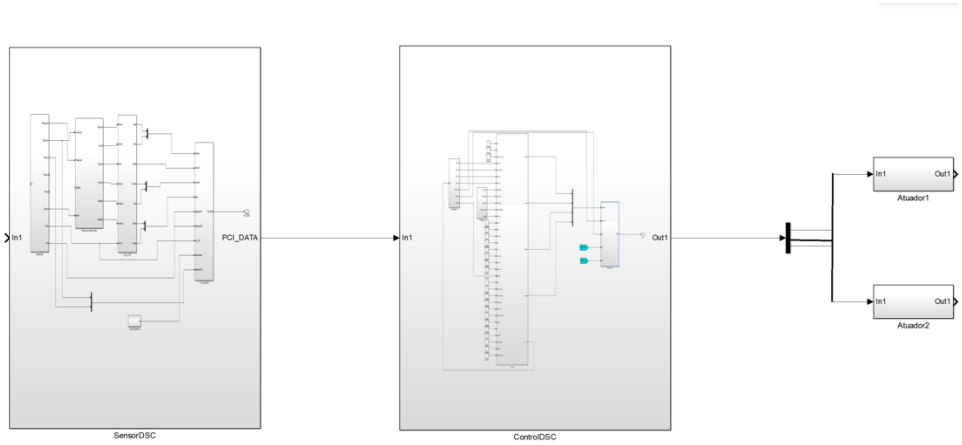
Since both industry and safety standards, especially in aerospace and automotive domains, have recognized the maturity and potential of model-based techniques in supporting system design and dependability analysis, model-based engineering became a reality in the development of safety-critical systems. Compositional dependability/safety analysis techniques, e.g., HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies), AADL Error Annex and AltaRica, provide the automated support for safety engineering, and seamless integration between system design and dependability analysis, which can be performed in a single model, contributing to reduce the complexity in performing system dependability analysis.

The design and dependability properties of a safety critical system might vary according to the targeted context of operation. Variation in the usage context may impact on the choice of redundant or non-redundant architectures in the system design. In dependability analysis, usage context variation may raise different hazards with different causes, different risk that the same hazard may pose for the overall safety, different component faults might occur and contribute to the occurrence of hazards, and different safety requirements (functional and non-functional) may be allocated to eliminate or minimize the hazard effects.

So we provide a systematic and context-aware model-based approach to support dependability analysis of unmanned aerial vehicles. The approach was built upon compositional dependability analysis techniques. The approach was applied to perform dependability analysis of a real-world Santa Cruz Low-Cost UAV GNC (SLUGS) automatic pilot developed in MATLAB/Simulink with the support of HiP-HOPS dependability analysis tooling. The application of the proposed approach reduced the effort, costs, and the number of errors in performing Hazard Analysis and Risk

Assessment (HARA), component fault analysis/modelling, and enabled the automated generation of FTA and FMEA dependability artefacts required by the standards to achieve safety-certification.

Advances in the approach to contemplate the security was done and a paper is in progress to be submitted to a Journal. The model that puts together Security and Safety can be seen in the next Figure. In this Figure the fault trees are put together. And the failure expression of a safety and security can be seen in Table. In this table we can see that security and/or safety failures together can provide Hazards.



Name	Failure Expression	Effect
Communication Lost	Denial of Service or Man in the Middle or Omission SensorDSC.ToControlIMCU or (LogicFailure at SPI board) or (Late.SensorDSC.SensorDATA or Omission.SensorData) and (Late.SensorDSC.ToControlIMCU or Omission.ToControlIMCU	Communication Lost between groundstation and UAV
Hijacking	Man in the Middle and (Value.SensorDSC.ToControlIMCU)	Value.WayPoints
GPS Failure	GPS-Spoof or (logical Problens.SensorDSC.SensorDataGPS)	Aircraft fall or location lost

2.10 Security policies, mechanism and strategies

Once defined the attacks and the possible problems and relation between safety and security (the influence of both to define or get a Hazard), we start to think in possible countermeasure. We know that cryptography is one of the possibilities to provide security, but we also know that the performance, mainly in critical embedded system can be a problem. So we start with physical solution.

Applications for Unmanned Aerial Vehicles (UAVs), operating in unlicensed bands, are vastly growing with the consolidation of the Internet of Things (IoT). However, those bands have become overcrowded as systems using them are continuously increasing. In this context, Cognitive Radio (CR) and spectrum sharing techniques have emerged as promising strategies to overcome the problem of spectrum scarcity in wireless networks, thus being considered as enabling technologies for the future 5G wireless networks. Thereby, the integration of CR with UAVs can bring important

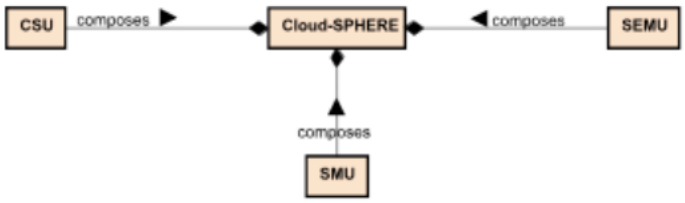
benefits for the massive deployment of UAVs. So we provide an overview on the state of the art of CR technology for UAV communication. Details can be obtained in \cite{ICUASCR_guilherme}.

For investigating the advantages of cognitive radio, Machine Learning techniques have been widely applied to predict primary users arrivals. However, the available simulators are usually complex and highly time consuming. Therefore, we proposed and validate a simple and intuitive primary user arrivals data generator, MARIO, that can produce random arrival data for multiple channels by employing Poisson process. This generator is validated by using the generated data to predict new sequences according to a Hidden Markov Model. Our results show that the data generator can be used to simulate various traffic patterns over different channels. To validate the generated data, we employed an HMM to predict unknown sequences by applying the training on the simulated data. The present study offers the opportunity of producing spectrum traffic data without the fall-downs of using a complex and, usually, counter-intuitive simulator.

Another approach to overcome the security problem was treated in parallel, the Cloud-SPHERE approach. Many opportunities arise for UAVs when considering their connection with other devices or systems. Many employed solutions can be improved, while new applications can be envisioned. At the same time, new challenges need to be overcome. The first set of challenges relates to public safety and privacy --- how to ensure the security of collected and distributed data, as well as the population privacy against snooping. The second set of challenges relates to standardization --- how to insert UAVs into the airspace and make possible for them to communicate with other devices seamlessly. The third set of challenges relates to technical difficulties --- how to overcome device heterogeneity and resource limitation in order to provide robust internal and external UAS communication.

In its current state, SPHERE is focused in the vehicle internal communication, that is, the communication between the vehicle core and its modules and clusters of modules. Cloud-SPHERE~extends the SPHERE platform to provide secure communication between UAVs and between the UAVs and the infrastructure, including the Internet and/or Cloud/Fog computing technologies (Cloud—SPHERE - (Security and safety Platform for HEteRogeneous systEms connected to the Cloud)). It also aims to support secure service provision, consumption and discovery, taking into account data sensitiveness and trust between devices. With that, UAVs can be securely integrated into the Internet of Things paradigm.

For that, Cloud-SPHERE'~CSU handles communication security tasks, and a new module handles service exchange tasks. Module SEMU (Service Exchange Management Unit) has its functionality distributed among SPHERE units to manage service registration, discovery and exchange considering security policies of data sensitiveness and trust between devices.



2.11 Energy Consumption

For battery-powered embedded systems like Unmanned Aerial Vehicles (UAVs), energy efficiency increases their autonomy, resulting in tasks being realized with less power. With less power being consumed during each mission, the battery will require fewer recharges, thereby increasing its lifetime and reducing the waste. Even though some effort has been done in energy efficiency for UAVs, most published papers focus on finding alternative energy sources for those vehicles. We proposed the Navigation Phases (NP) platform, which provides a very well-defined way of controlling the behaviour of UAV's internal components during a mission.

The main concepts of NP are provided, as well as the results of an initial prototype for controlling the component's behaviour through different mission stages. For battery-powered devices such as UAVs, energy efficiency increases the vehicle autonomy, and also potentially increases the battery lifetime and reduces waste.

The NP platform can be expanded with other control parameters besides the ON/OFF state, such as bandwidth and radio power, for example. A feedback on the commands would also improve the system's safety and point to potential problems or attacks. Artificial intelligence strategies can be applied together with NCI and Cloud--SPHERE platforms for identifying and acting on emergency situation.

3 Final Considerations

In this report we presented a summarized overview of the research done in the context of GRANT W911NF-18-1-0012. We provide the state-of-the art regarding the security of unmanned vehicles connected to the Internet, Cloud or similar network discussed through the results of a systematic review. Results show very few security mechanisms employed in this scenario, emphasizing the need of security-aware solutions for connected UAV networks. Also we provide initial models for the integration between safety and security in the IoMoT context.

The results presented are a step forward in the state-of-the art and is the beginning of the investigation. We also presented a model-based approach to support unmanned aerial vehicles dependability analysis/modelling. Such approach enables safety analysts performing dependability analysis aware of the impact of the variation in the design choices and usage context. We have also shown that the usage of model-based techniques contributes to reduce errors in performance dependability analysis through automatic synthesis of dependability artefacts required for certification of autonomous vehicles. Further works intend to investigate the analysis of the impact of the context on Software In the Loop decomposition, the usage of existing model-driven techniques to support the generation of assurance cases from HARA, component failure data, FTA and FMEA.

As future work We intend to perform a study to analyze the interactions between security and safety mode in deep, and the usage of Bayesian Networks (BN) to improve the analysis of the relationships between safety/security in the unmanned aerial vehicles domain among other things. We are also planning to work with STRAUSS (reSilienT aiR tAxis architectUre for Smart citieS) - The main goal of STRAUSS is to extend STUART to propose a fault-tolerant and robust system for air taxis that can adapt their planned mission dynamically by sharing information with the ATS system. In a distributed way, air taxis can only decide of an action locally i.e., when they are confronted to the adversity and cannot anticipate it. Communications with the ATS system are necessary to optimize the course of actions that air taxis have to do when an adversity occurs in their neighboring.