Requirements and Challenges for Secure and Trustworthy UAS Collaboration

Marco Anisetti, Claudio A. Ardagna
DI, Università degli Studi di Milano
Milan, Italy
{firstname.lastname}@unimi.it

Barbara Carminati, Elena Ferrari*
DISTA, Università degli Studi dell'Insubria
Varese, Italy
{firstname.lastname}@uninsubria.it
* corresponding author.
All authors have contributed
equally to this work.

Cora Perner
Airbus Cybersecurity GmbH
Munich, Germany
cora-lisa.perner@airbus.com

***Abstract*—Integration and increased uses of unoccupied aerial systems (UAS) challenge current airspace operation. Rather than centralised airspace management (which is rapidly reaching capacity limits), those vehicles need to collaborate safely and efficiently. However, the vehicles differ significantly with respect to capabilities, carried equipment, and certification requirements. The main focus of this paper is how to determine a safe level of interaction in a heterogeneous network, where not all vehicles are (equally) trustworthy, but cooperation is required for many different reasons (e.g., collision avoidance, implementation of collaborative tasks). Consequently, this paper presents the main research challenges deriving from integrating UASs in a shared airspace, with a focus on the demanding scenario of urban air mobility. Specific use cases are described to highlight the main challenges and requirements for a security architecture. Furthermore, a roadmap is presented towards addressing the main challenges: trust estimation, interaction adaptation, controlled information sharing, and continuous monitoring and adaptation.**

***Index Terms*—UASs, Urban air mobility, Trust, Secure collaboration, Continuous monitoring and adaptation.**

I. Introduction

Unoccupied aerial systems (UASs) are technologically more advanced unoccupied aerial vehicles (UAVs), i.e., flying vehicles without a human pilot on board. Consequently, when analysing UAVs/UAS, one also has to consider the equipment needed to control and operate them, including all architectural components of a flight control system, such as, ground control stations (GCSs), communication links, and payloads. UASs, due to their increasing affordability, have recently gain attention and their use has been proposed in many domains, including agriculture, oil, gas, and electricity utilities, the media, safety and disaster management [1], transportation of goods [2], [3] and (in the future) people [4], to name but a few. However, this increased popularity brings new challenges that current air traffic management (ATM) and air traffic control (ATC) are not equipped to handle. Today's airspace is already operating near or at capacity [5], [6]. Consequently, novel means are required to separate UASs from existing private and commercial traffic, and from each other. In response to these needs, significant research efforts, such as, those by the Single European Sky Advanced Research Program [7], have been undertaken. To allow efficient and safe collaboration among UASs, the following steps and challenges need to be taken into account:

- *Detecting the incoming vehicles.* Both airworthiness authorities and researchers have suggested to mandatory fit UAS and other aircraft with transponders [8], [9], [10]. However, the commonly suggested Automatic Dependent Surveillance-Broadcast (ADS-B) protocol does not include security provisions (such as authentication) [11]. Hence, finding a secure alternative is still a rewarding topic for research.

- *Establishing a secure communication channel.* After successfully detecting an incoming vehicle, a secure communication channel needs to be established. As commercial aircraft may be operated for several decades, the air traffic control network includes many legacy components from as early as the 1960s. Moreover, any new technology that is being introduced will be in service for a similar time frame. Consequently, it is paramount that update-ability and interoperability are considered in the design. Moreover, aircraft components have to undergo a lengthy certification process. This makes it a particular challenge for security applications, which typically have a much shorter development and deployment cycle.

- *Determining the level of interaction*. This requires to determine how to organise communication in an environment where not all vehicles are (equally) trusted. The earliest example for 'trust in aviation' research is [12] and focused on the human aspect of trust.

The main focus of this paper is on the last point and aims to discuss gaps, challenges, and possible approaches to trustworthy coalitions and collaborations. Specifically, we are looking at the integration of spatial policies and trust assessment (see Sections III and V), and assurance monitoring and adaptation (see Sections VI and IV) into a coherent approach, thus determining a safe level of interaction. In standard IT communication, untrustworthy partners can simply be excluded from the communication. Yet this is not an option in aviation. To avoid coming into conflict (i.e., close enough that a collision is only avoided by luck) with each other, we need to communicate even with untrustworthy or partially trustworthy vehicles. Notwithstanding, trust assessment can be

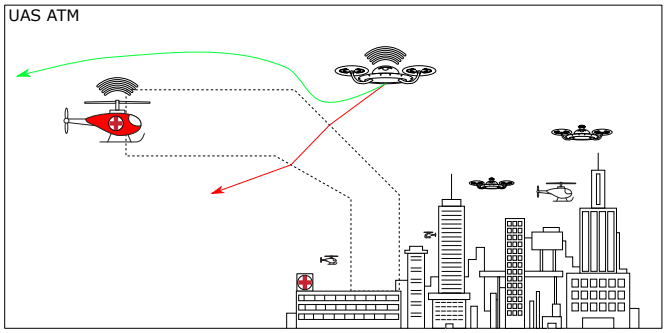

Figure 1. Reference UAS Scenario, adapted from [13]

used to determine the operations a vehicle is authorized to do and the adaptation activities to restore to a higher trust level. For instance, UASs could envisage sharing only the most basic position data (similar to a transponder) with an untrustworthy vehicle, while more trustworthy ones are provided with more detailed data, such as fuel status. Moreover, an interaction with an exploited/infected vehicle can cause an attack to quickly propagate throughout the entire network, with significant ramifications on safety, also for nearby passenger aircraft. Hence, the vehicles need to establish a level of collaboration that is safe *and* secure.

This scenario is further complicated by the lack of assurance processes for UAS; for instance, unlike larger aircraft, they do not need to follow a stringent certification process. Consequently, the vehicles are cheap, easy to obtain, and easy to use. In addition, they do not have significant computation power, thus preventing the use of some more advanced security functions.

This paper analyzes the problem of trustworthy and secure UAS collaborations. To this end, a reference scenario is given in Section II. The requirements for a secure collaborations among UASs are analysed along four main viewpoints: i) trust estimation (Section III), ii) controlled information sharing (Section V); iii) continuous monitoring and assurance (Section VI); iv) interaction adaptation (Section IV). For each point, existing challenges and possible countermeasures are discussed. A mapping between use cases in Section II-B and challenges/actions in Sections III, IV, V, VI is provided in Section VII. Finally, Section VIII concludes the paper.

II. Reference Scenario

Our reference scenario is urban air mobility, one of the most challenging scenarios with operational aspects relevant within the next 5-15 years. As depicted in Figure 1, this incorporates various type of aerial vehicles (e.g., helicopters, UASs) of varying degrees of autonomy that operate concurrently in an urban environment. As air traffic control is already operating at capacity, the vehicles have to autonomously and collaboratively plan their route. This includes avoiding collisions with each other and independently choosing landing sites, when/where to refuel, to name but a few. Furthermore, the vehicles also have to clear corridors for emergency services as well as for vehicles in emergency conditions, such as after suffering a bird strike. The latter is much more frequent in an urban environment where, unlike airports, no measures are being taken to discourage birds.

This scenario clearly demands for secure collaboration among UASs. To better understand its requirements and challenges, we need to first briefly introduce the vehicle capabilities (see Sec. II-A), which (aside from size) differ significantly from each other with respect to capabilities and applicable requirements. Also, we provide three use-cases for the urban air scenario (see Sec. II-B), to better contextualize the identified requirements.

A. Vehicle capabilities

The key distinction with respect to capabilities is the level of autonomy that the vehicle can provide, as this also influences technical equipment (such as sensors). Consequently, the following types of vehicles can be distinguished, with increasing automation: (1) Human piloted vehicles; (2) Remotely piloted aerial systems; (3) Partly autonomous vehicles; (4) Autonomous aerial vehicles.

At the most basic automation level, humanly piloted vehicles are controlled by an on-board human pilot. Any automation is only there to *support* the pilot. However, this pilot needs to be aware of other airspace users to avoid collisions and negotiate landings, for example at heliports.

The next level of automation is a remotely piloted aerial system (RPAS). Here, the pilot remains on the ground, and controls the vehicle via remote links using either dedicated hardware or a handheld device. The vehicle may either be operated in visual line of sight (VLOS) or beyond (BVLOS). Depending on the manufacturer, the command and control link (C2) between the vehicles can be implemented in the radio frequency spectrum, a proprietary implementation in the WiFi band, or via 5G. While larger BVLOS operations may also include satellite communications, those are considered to be out of scope for an urban air mobility scenario. For redundancy, more than one antenna/link may be used. Moreover, the control of a vehicle may be passed between ground control stations/controllers during the journey. For safety reasons, such vehicles may be able to perform some functions automatically, such as land if the link to the controller is lost or if the power supply is critically low.

Going beyond that, partly autonomous vehicles can perform (parts of) missions without any human interaction, but have a human in the loop that supervises one or several vehicles and can take over if needed (e.g., if a sensor fails) in challenging weather conditions or for critical flight phases.

The final level are autonomous aerial vehicles (AAV) that operate without any human intervention whatsoever.

All those vehicles need to interact with each other as they share a congested airspace. Thus, at the most basic level, collisions have to be avoided. As even a collision between two unoccupied vehicles could result in debris hitting the ground, this application is highly safety-critical. To avoid this, various types of vehicles need to exchange information.

B. Use Cases

Within the urban air scenario, there are several use-cases that can be considered (cf.[14]). We have selected the following three as they represent cases requiring different levels of collaboration.

1) Collision Avoidance and Path Planning: On the most basic level, let us consider collision avoidance and path-planning, that is, finding the shortest collision-free route to a destination. This is already a complicated problem without considering security. However, for safety reasons, we need to ensure that claims of other vehicles are legitimate. One possible attack could be a spoofed signal of another vehicle that aims to exhaust the power reserves of a vehicle by claiming to fly into conflict. Obviously, such a behaviour should lead to a loss of trust in the involved vehicle. Moreover, if such a behaviour is detected, it might be necessary to warn nearby vehicles. Notwithstanding, for safety reasons, collision avoidance needs to be performed efficiently irrespective of trust levels.

2) Emergency management: As a variation of the above, let us now consider that one vehicle encounters an emergency and needs the quickest possible route to the nearest landing site. Similar problems arise also in case of an emergency vehicle that requires priority. Here, vehicles need to give way while taking their individual constraints (e.g., speed, power available) into account. It can be assumed that emergency vehicles will be equipped with some sort of authenticated transponder[1] to indicate priority (similar to the familiar flashing lights and sirens). However, this assumption does not hold for vehicles that suffer an in-flight emergency. Consequently, other vehicles need to determine whether the emergency communication is genuine, and react accordingly. While the signals from emergency vehicles are trustworthy, emergency signals from other vehicle types may not be. On the other hand, it is necessary for flight safety that other vehicles move out of the way of a vehicle that can no longer manoeuvre.

3) Formation Flight: To simplify the path planning problem and increase airspace capacity, several vehicles will group into (temporary) formations with reduced separation between them. Here, all vehicles in the formation need to agree on a policy with the vehicle that wants to join the formation. Subsequently, n of the nearest neighbors will monitor the vehicle's behaviour and trigger a warning to the existing formation to break away. At the same time, all other vehicles of the formation also need to be monitored for anomalous behaviour, both with respect to security (e.g., privilege violations) as well as safety aspects (e.g., loss of power). While it will be necessary that vehicles alert their neighbours of any problems they detect, some level of monitoring also need to be implemented on neighbouring vehicles, in case the vehicle itself is unable to report. While usually only trustworthy vehicles will be allowed to join a formation, the level of trust may change during the operation, which may require a physical or cyber reaction.

[1]An automated transceiver (integrated transmitter and receiver) that emits an identifying signal upon query

C. Secure collaboration among UASs

The above use cases well highlight that, to avoid collisions, some degree of collaboration is needed. They also emphasise that the level of interaction has to be differentiated based on the safety and security provisions of other aircraft. For example, the minimum separation between vehicles providing very accurate position data will be lower than that of a vehicle with very low navigational accuracy. Thus, for the establishing of a secure collaboration among UASs, it is crucial to have trusted information on involved vehicles. This is the biggest challenge to overcome. In this heterogeneous environment, it is logical that the vehicles provisions will not be homogeneous.

This challenge starts with the certification process. A recent concept paper of the European Aviation Safety Agency (EASA) [15] suggests to certify the following categories of UAVs/UASs, comparable to the approach that is used for today's occupied aircraft: (1) Transport of people; (2) International cargo operating under instrument flight rules; (3) Transport of cargo in urban environments above people.

However, other types of aerial vehicles that operate in an urban environment (such as those used for inspection or by private parties) have no mandated airworthiness certificate. Consequently, there are no minimal standards that need to be adhered to and that other airspace vehicle can rely on being fulfilled.

Beyond that, even the vehicles that *are* certified will not adhere to a common standard. Especially for larger vehicles, the certification process is lengthy (and thus expensive). Likewise, any update to an existing system is a lengthy process, as it needs to be proven that the modifications do not interfere with safety properties.

Together with the fact that larger vehicles will likely remain in use for several decades, challenges related to security arise. On the one hand, security is needed to achieve safety (e.g., by ensuring that only authorised users can control a RPAS). On the other hand, safety requirements result in delays of adapting new security standards (e.g., patching of security vulnerabilities, adaptation of new encryption standards). Hence, aerial vehicles operate in a highly heterogeneous environment with respect to security standards.

To cope with this highly dynamic environment, we envisage the need of an approach able to dynamically manage and adapt the level of UASs collaboration based on vehicles trustworthiness. Thus, before any interaction could be considered, a trust estimation for a UAS has to be performed (see Sec. III). Subsequently, the appropriate policy that determines the interaction has to be selected (see Section V). Throughout the entire interaction, the other vehicle has to be monitored (see Section VI), both with respect to physical characteristics (e.g., to verify whether it keeps its course) as well as with respect to information exchanged (e.g., to verify whether it tries to access data of another vehicle). If any divergence from expected behaviour is noted, the interaction has to be

adapted accordingly, such as, by breaking up a flight formation (see Section IV). However, it should be noted that safety takes precedence over security in aeronautical applications. Consequently, vehicles may need to interact with untrusted vehicles to avoid a collision. An appropriate policy for minimal data sharing will likely be mandated by airworthiness authorities and could for instance consist of a transponder signal indicating speed, course, and altitude.

In the following sections, we analyse the main requirements of each step of this comprehensive approach to establish and achieve a secure collaboration among various UASs.

III. Requirement 1: Trust Estimation

As we have seen in the previous section, it may be often the case that UASs need to establish a level of collaboration in a scenario where not all vehicles are (equally) trusted, or where the current level of trust is unknown or may dynamically change. There is therefore the need for a trust management mechanism able to estimate the level of trust of an unknown UAS on-the-fly, or to adjust a previous estimation, so as to assign it a risk level and, based on that, plan future actions (e.g., changing the route) as well as possible levels of collaboration.

Trust computation and management has been subject of extensive studies in many different domains [16], such as electronic commerce, recommendation, multi-agent systems, as well as centralized and decentralized social networks [17].

Trust issues have also been addressed for IoT ecosystems from different perspectives. For instance, [18] surveys trust computation models that have been developed for IoT systems for the purpose of service management, i.e., whether or not to select an IoT device as a service provider, whereas [19] focuses on protocols ensuring trusted communications among IoT devices. Durresi et al. [20] proposed a general measurement-based trust management framework for IoT, where trust is modelled through trustworthiness and confidence metrics. Both human-to-devices and devices-to-devices trust relationships are considered. More recently, blockchain-based solutions have emerged. For instance, Tang et al. [21] proposed a blockchain-based trust framework for cross-platform collaborations of IoT devices, where each interaction among devices is signed by the participants and recorded on the blockchain.

However, despite the many proposals that have been published so far, the definition of a fully distributed, scalable, and dynamic approach suitable for the IoT context is still missing.

Trust is also increasingly being investigated in the field of autonomous systems. According to a recent survey [22], the research has mainly focused on trust between humans and fully or semi-autonomous systems, for instance self-driving cars. As far as UASs are concerned, [23] addressed the issue of trust-based communication protocols, whereas [24] proposed a reputation-based auction mechanism to select UAV operators. Beyond this, [25] proposed a system to determine the trustworthiness of messages used in UAV-to-UAV (U2U) and UAV-to-infrastructure (U2I) communication. Furthermore, [26] leveraged on genetic algorithms for trust estimation in the scenario of flying ad-hoc networks (FANETs). The proposed model has been extended in [27] by adopting a multicriteria fuzzy classification method to deal with the behavioral uncertainty of FANET nodes. However, the research in the UAS domain is still in its infancy, and many open challenges have yet to be addressed. Some of the most relevant ones are discussed in the following subsection.

A. Challenges

- **C1.1: Multi-factor trust estimation.** Trust estimation in our reference scenario should rely on different dimensions. First of all, it should rely on both static information about UASs (such as UAS type, adopted protocols, configurations, manufacturer, organization to which the UAS belongs to), as well as on dynamic information: (i) past and present behaviors of the UAS, and (ii) past interactions. For instance, if previous interactions were successful, this might increase the trust level w.r.t. a UAS that it is encountered for the first time. Clearly, the more information is available about the interacting UAS, the more precise the trust level estimation is. For instance, if we have information about the route followed so far by the UAS and the actions it has performed (e.g., number of stops), we can use this information to detect an anomalous path and therefore diminish its trust level accordingly. If information on the UAS flight plan and its mission (e.g., successful delivery, traffic monitoring, emergency response) are available, it can be checked whether the position of the UAS is compatible with its declared mission and/or flight plan.
- **C1.2: Context-aware trust estimation.** One important challenge in our reference scenario is the inclusion of contexts in the trust management process [**?**]. Indeed, contextual information may influence trust computation in many different ways. For instance, it may impact the weight given to the various dimensions that the trust computation model considers (e.g., in emergency situations some aspects are more relevant for trust computation than during normal operations). Moreover, context similarity can be exploited as a way to obtain a faster trust computation. For instance, when a UAS encounters a new context (e.g., a new area) it can leverage on trust estimations done in the past in similar contexts to compute the trust level of UASs it may encounter.
- **C1.3: Imprecise trust estimation.**
  One of the more challenging aspects in our reference scenario is that not all the information for a correct trust estimation is available when needed. Moreover, mechanisms should be put in place to estimate the trustworthiness of the information about the UAS on which trust estimation relies. As such, we need a trust mechanism that can adapt to the lack of some information and/or to different level of trustworthiness of the information sources. In this context, another important aspect concerns the trustworthiness of data, which might be affected

by measurement errors, failures and malfunctioning, and attacks.

- **C1.4: Efficient trust estimation.**
  Trust estimation should be very fast, as UASs interaction often requires to take critical decisions in very short time. A further design issue is who is responsible for trust computation.

B. Actions

Trust computation in UAS systems is a challenging task which requires to address several important challenges, which have been described above. This requires to plan a set of actions that span different aspects of trust computations.

- **A1.1: Decentralized trust computation.** Ideally, for UAS, trust computation should be centrally managed by the ground-based controller that can rely on historical data and enough computational power to perform the computation (e.g., making use of machine learning algorithms). However, there could be cases in which it is not possible to communicate in real time with the ground-based controller or where one is not available. In such a case, if the UAS has enough computational power, it must be equipped with tools that can perform the computation by only relying on the information it has to obtain an estimation of the trust level. Additionally, pushing some computations on the UAS can also be useful for timely adjustments of the trust level, as well as to optimize resource usage. As such, the trust management system should be implemented so that it can rely on both the UAS and the ground-based controller for trust computation. Additionally, it should be designed to be resilient to temporarily loss of connectivity between the UAS and the controller.
- **A1.2: Dynamic trust adaptation.**
  UAS must be equipped with tools to dynamically change the trust level of UASs, for instance to react to a change on its behavior, which may lead to an increase or decrease of the trust level. This ability to change the trust level over time requires new solutions that dynamically evaluate the status of UASs and corresponding collaboration groups, as well as new solutions to adapt their behavior at run time (see also Section IV).
- **A1.3: Autonomous trust-based decisions.** UAS must be equipped with tools that make UASs able to autonomously take decisions based on the computed trust level (e.g, emergency landing or change of the route), when communication with the ground-based controller is not possible, no controller is available, or to limit the communication traffic between the controller and the UASs.

A further action is related to data trustworthiness, since the trust computation process should rely on correct and secured data (see Action 4.2 in Section VI) as much as possible.

IV. Requirement 2: Interaction adaptation

Once trust estimation has been performed, it should be used to determine which level of interaction can be established with a given UAS, if any. The level of interaction is critical since the planning of different actions (such as sharing a small corridor, landing or flying at close range) can be based on UAS interactions.

In case of very low trust levels, the UAS might stop any form of interaction, as it may be hazardous. Consequently, it will try to move out of the way as quickly as possible to mitigate any risk (e.g., changing the flight route, stop the flight). Otherwise, the trust estimation should drive the interaction by establishing whether some specific data should be exchanged. For instance, just the most basic positioning data can be communicated to a UAS that is not fully trusted (e.g., by reducing resolution of position accuracy), while telemetry data and flight plan data are not. In the case of more trustworthy vehicles, more details can be provided. Clearly, the level of interaction should be also driven by the kind of operations the UASs are performing. In case of very critical operations, it may happen that it is worth taking the risk of collaborating with not highly trusted UASs, if this is the only way to carry on the mission or necessary for flight safety. For instance, in case of an emergency, fuel status can be exchanged among the UASs in order to better coordinate a specific urgent intervention. In contrast, this risk should not be taken for less critical operations (e.g., delivery of goods). Another aspect that should be considered is the freshness of the UAS trust level as well as the trust level history associated with a specific UAS. For instance, in order to determine the level of communication, the time elapsed since the last trust evaluation for a given UAS, and how often this UAS has recently been considered untrusted should be considered. In some scenarios, it can be preferable not to communicate sensitive data to a UAS that was often considered to be not fully trusted, for instance due to the difficulties to be updated in case of vulnerabilities (e.g., only one update per month) In general there is the need to have a set of continuously updated metrics on the trustworthiness of the UASs that can capture the evolution of UAS trust level over time. Such metrics, that can be customized according to the reference scenario, can be then used to fine tune the decision on what to exchange during a communication. Finally, it is important to stress that these types of decisions on the level of communication cannot rely on human intervention, but they should rather be taken instantaneously and autonomously by the UAS. This means that there must be a system capable of dynamically adapting the communication level to the computed trust levels, the scenario, and data to be communicated.

A. Challenges

The adaptation of interaction levels depending on the UASs trustworthiness introduces new challenges summarized as follows:

- **C2.1: Adaptation to different scenarios.** Communication between UASs is essential in many contexts. The

idea of not communicating with a not fully trusted UAS cannot be considered in all the scenarios where UASs are used. It is fundamental to identify scenarios of usage and the corresponding acceptable level of trustworthiness for a given set of data to be transmitted. This process is challenging since scenarios and trustworthiness values can dynamically change over time, and this may lead, for instance, to the interruption of a given established communication. An adaptation process should be able to adapt the communication level to a changing context and a changing trust level of the involved UASs.

- **C2.2:Temporal metrics.** Being computed based on specific properties, the trust level is a temporal property of a UAS that can vary over a time frame. Being capable to evaluate how such trust level evolves in time can permit to predict critical situations in advance and better support communication adaptation in critical scenarios where a decision can benefit by a more refined analysis on the UAS trustworthiness.
- **C2.3:Decision system.** The definition of adaptation metrics is challenging as well as the definition of a decision system that evaluates them in order to reach a concrete decision on the communication of data. In addition, such decision should be based also on the contextual scenario and tailored on the type of data to be exchanged, for instance considering the sensitivity of the data to be communicated in that specific context. For instance, in case of an ongoing communication, a decision on how to proceed is critical as well, and should consider the communication status and what has been communicated in the past.

B. Actions

It is important that the system is equipped with communication adaptation mechanisms that allow to adapt the communication content to a changing level of trust and scenario of usage. It is also important to monitor the evolution of the trust level via temporal-related metrics that support the communication decisions in critical situations allowing predictions. Such challenges can be broken down in few actions, which assume high priority in UASs.

- **A2.1: Monitoring of trustworthiness.** In the framework of a complex and changing cybersecurity landscape, the trustworthiness itself should be considered as temporal variable properties that should be monitored with metrics that can capture the important behaviours. For instance, how frequently a UAS shows a low trust value in a given context.
- **A2.2: Implementation of automatic communication adaptation.** It is not feasible that any adaptation requested by a specific situation passes trough a human decision process. Therefore, the UAS itself needs to make a decision based on the trust metrics, situation, and type of data to be communicated.

V. Requirement 3: Controlled information sharing

Once the interaction level has been computed, collaboration can be established and this will enact different levels of information sharing among the involved UASs. Such information sharing should be timely and controlled, in the sense that only information needed for the collaboration should be shared and only when indeed needed. In general, controlled information sharing is achieved through the adoption of access control policies and related checking mechanisms, whose purpose is to prevent any action deriving from unauthorized accesses. Access control policies and related mechanisms have been the subject of extensive research [28] since the '70s, with the result of the proposals of several access control models (e.g., discretionary access control - DAC, mandatory access control - MAC, role-based access control - RBAC, attribute based access control - ABAC) adopted in different commercial data management systems (e.g., DBMSs, operating systems). The access control problem has been further investigated in several innovative scenarios since, like in the web (e.g., [29], social media (e.g., [30]), and, more recently, in IoT/sensor networks (e.g., [31]).

Information sharing has also been investigated in the framework of multi-UASs collaborative tasks. Several works have investigated this problem, aiming at design solutions to efficiently and effectively share information needed by a UAS team to achieve a common goal (e.g., real-time path planning). As an example, in [32], [33], authors answered questions on which information has to be shared and how the gathered information has to be fused, in order to enable UASs cooperation.

However, to the best of our knowledge, the designed information sharing was supported without any security mechanisms, as security was not the main driver.

In contrast, we believe that information sharing supporting collaborations among unknown UASs, should leverage on the encoding and enforcement of proper sharing policies, that should state which information should be shared for how long and to which level of details, on the basis of the computed level of interaction.

A. Challenges

- **C3.1: Expressive sharing policies.** As identified in challenge C2.1, the interaction level depends on the target scenario. This holds also for the underlying information sharing. As such, policies should be heavily context-dependent, in that the policy enforcement process should take into account the context where information sharing should take place (e.g., emergency vs normal situations, number of other UASs in the area, location and time of the information sharing request). Policies can also mandate, depending on the scenario, additional operations to be done in association with policy enforcement. Such operations are usually referred to as *obligations*.
- **C3.2: Efficient policy enforcement**. Another important requirement is that the enforcement monitor in charge of

make data sharing compliant with the specified policies should be very efficient, since information sharing may be subject to tight time constraints and dynamic adjustments. Policy enforcement should be able to immediately react and adapt the information sharing process, as soon as the trustworthiness of an UAS changes, and, as a consequence, also the previously determined levels of interaction.

- **C3.3: Trusted and resilient policy enforcement**. In general, access control mechanisms rely on a trusted entity for policy enforcement. This plays the essential role of verifying each authorization before any data release/usage. Assuming a trusted entity in UASs scenario might be a challenge. Even in case the UASs can rely on trusted ground-based controllers for policy enforcement, it should be as resilient to a loss of connection between the UASs and the ground-based controllers as possible.

B. Actions

In order to design a timely and controlled information sharing for UASs, we identify the following actions:

- **A3.1: Policy modelling**. The first action is the identification of a proper access control model and language through which the UAS access control policies supporting the required expressiveness (challenge C3.1) can be stated. Literature offers several standard models and related languages. This action requires to analyse the state of art, select the most suitable model/language, and adapt it to the UAS scenario.
- **A3.2: Automatic policy instantiation**. Once the interaction level has been determined, a set of new policies defined according to the adopted model/language has to be instantiated. This task should be done automatically by UASs. The process should be resilient to a loss of connections with ground-based controllers. It should also be resilient to attacks done with the aim of instantiating an incorrect policy set (e.g., resulting in weaker constraints on information sharing).
- **A3.3: Efficient and resilient policy enforcement**. As soon as the policies have been deployed, the ongoing information sharing has to be compliant with new authorizations. This implies the definition of a very efficient reference monitor (i.e., the module in charge of policy enforcement) able to be continuously aware of new policies deployment, as well as of the revoking of active policies, and to immediately react by regulating the ongoing information sharing accordingly. The design of this efficient reference monitor should be tailored to the UASs hardware and software limitations.

VI. Requirement 4: Continuous monitoring and assurance

UAS collaborations are highly dynamic and their security status evolves quickly. The security of a collaboration depends on different aspects, including the behavior and configuration of single UASs, as well as contextual events or interference from external attacks. Continuous monitoring and assurance evaluation are mandatory in this scenario and provide the basis for a continuous evaluation of the trust of the UAS collaborations. They also represent the basis for a dynamic policy checking, where changes in trust levels may result in different sharing policies to be checked.

In the last few years, continuous monitoring and assurance have received increasing attention in the development of trustworthy cloud-edge systems. This has been mainly because the need of evaluating non-functional properties, with security at the forefront, has become more stringent than ever. Continuous evaluation and assurance aims to increase the confidence that a system behaves as expected despite failures and malfunctioning. Assurance techniques have been primarily defined for service-oriented architectures and then more recently applied to cloud computing (e.g., [34], [35], [36], [37]. Recently, research on continuous monitoring and assurance has started to also focus on cloud-edge systems and IoT. Ardagna et al. [38] discussed challenges in the design and development of assurance techniques for IoT and presented an architecture for assurance evaluation. Beyond that, Sato et al. [39] proposed an architecture for evaluating IoT trust, where the trust level considers device identification, monitoring of device behaviors, device connection processes and protocols. Furthermore, Taherizadeh et al. [40] presented a survey on the monitoring of self-adaptive applications, based on decentralized edge computing. In addition, Ardagna et al. [41] proposed an approach for the evaluation of the trustworthiness of data collected in IoT/edge environments. Approaches based on remote attestation have been also presented to prove the behavior of a device and establish an according level of trust. Finally, continuous monitoring and assurance have been increasingly discussed in the context of UAV/UAS. Different surveys (e.g., [42], [43], [44]) presented how security and privacy are not the only concerns limiting the UASs application. As UAS are permeating urban areas, their increasing proximity to humans require strict safety assurance.

A. Challenges

Continuous monitoring and assurance of UAS collaborations introduce some new challenges that are summarized in the following.

- **C4.1: Hybrid and complex systems.** Today's distributed systems are incorporating a plethora of technologies including cloud/microservice architectures, edge networks and nodes, and a multitude of resource constrained sensors. These components/systems are heterogeneous and their lack of interoperability exacerbates the problems of guaranteeing safety, security and correct system behavior. This scenario is put to the extreme in UAS collaboration in an urban environment. In this context, there is the need of continuously evaluating UAS non-functional properties by means of a proper assurance approach, and this represents a key enabler for next-generation UAS systems.
- **C4.2: Untrusted providers.** Security of IT systems hitherto relied on the assumption of having trusted providers

and trustworthy evidence on the behavior of the system. This assumption is not sound anymore, especially in a UAS scenario, since UASs may be managed by unknown providers, breaking the trust relationships that hold in traditional IT systems. A proper monitoring and assurance technique must be able to evaluate the trustworthiness of a specific UAS and its sensors, as well as the trustworthiness of the collected data.

- **C4.3: Modeling of the behavior.** The modeling of a system/service/sensor behavior has been recently used to verify the correctness of a process and evaluate the reliability of a given system. Poisoning and adversarial techniques have been presented to transparently change the behavior of a specific system in a way that is not noticed by the system and its users. The problem is especially relevant in a UAS collaboration where an attacker might disguise a hostile UAS as a delivery UAS.

B. Actions

Guaranteeing continuous monitoring and assurance of UAS systems, especially when collaboration is foreseen, is mandatory for their success. Continuous evaluation in fact aims to maintain control over the whole system evolution while trying to reduce the risk of failures, malfunctioning, attacks, which could potentially have an effect on human safety. Continuous monitoring and assurance can be broken down to a few actions, which assume high priority for UASs.

- **A4.1: Behavioral monitoring.** Trustworthiness of UASs and their sensors is fundamental to build a chain of trust on a collaboration implemented based on their jobs. UASs often work according to missions (either individually or in a formation) and are often supposed to act according to predefined behaviors. The behavior of a specific UAS however could change over time and could be an indicator of a compromise or malfunction. In addition, the behavior of a single UAS can affect the entire formation, and it is therefore important to continuously monitor UAS behaviors to identify any deviations from the expected behavior early. Assurance and monitoring solutions tailored to the UAS scenario are mandatory to provide a trustworthy ecosystem.
- **A4.2: Data trustworthiness.** UAS collaborations rely on the exchange of data at high rates. Coordination and collaboration among UASs put strong requirements on the quality of data, as inaccurate data could lead to failure conditions. For instance, a GPS malfunction and resulting deviation from the flight path could cause a collision in a close formation. New approaches must be defined to verify the trustworthiness of data both validating UAS configurations, contextual data, and behavior parameters (see previous action).
- **A4.3: Attack resilience.** UAS collaborations are increasingly at risk of becoming the target of new attacks. They often implement high-value services, while being exposed to attacks and to resource exhaustion. Continuous monitoring and assurance must then evaluate the risk of an attack, providing solutions for early identification of the compromise, as well as the ability to quickly identify poisoning attacks aiming to disrupt the functioning of a UAS collaboration.

VII. Roadmap

In this section, the use-case specific security challenges described in Section II are mapped to the requirements, and correlated challenges and actions discussed in Sections III, V, VI, IV), with the according references to the corresponding items. This allows to build a comprehensive overview of the most important aspects of UAS security, thus leading to the development of a roadmap.

In Table I, issues that need to be addressed in all use cases are collected. All use cases require autonomy, both for occupied and unoccupied system elements. In occupied aircraft collaborating with UASs in a shared airspace as required in our scenario, it is necessary to reduce pilot workload (and thus the chance of mistakes with potentially serious consequences) as far as possible. Hence, the necessary processes should be performed automatically and ideally autonomously, thus require as little pilot interaction as possible. While the pilot should be informed of the current security status (for situational awareness, actions on their behalf should only be required when other mechanisms fail, e.g., to avoid a collision with an uncooperative UAS. The demand for autonomy also requires that the enforcement of decisions is efficient and resilient against external disturbances. This includes both accidental (e.g., due to malfunctions) and intentional (i.e., attacks) failures. Beyond that, the vehicles that are used to satisfy the use-cases are general purpose, off-the-shelf and not specifically adapted to the urban scenario and the challenges it brings. For example, a vehicle used to deliver emergency medication to a remote area may start in the city but then move to a more remote area and adapt its communication policies during the flight.

Table I
General Roadmap

Challenges	Requirements	Reference
Autonomy	Autonomous decisions	A1.3
	Efficient enforcement	A2.2
Stability	Attack resilience	A3.4
Adaptability	Adaptation to scenarios	C4.1

Table II
Collision Avoidance and Path Planning Roadmap

Challenges	Requirements	Reference
Spoofed signals	Efficient trust estimation	C1.3
	Efficient policy enforcement	C3.2
	Untrusted providers	C3.2
Monitoring	Efficient policy enforcement	A3.2
Misleading signals	Monitor trustworthiness	A2.1
	Monitor behaviour	A3.1
Missing signals	Modelling of behaviour	C4.4

Table II shows the mapping from challenges related to collision avoidance and path planning to requirements for efficient trust management.

The challenges are derived from the overarching need to collaborate efficiently with vehicles that are not a-priori trustworthy. Unlike in traditional computing, the interaction with a party cannot be rejected. Collisions must be avoided irrespective of whether that vehicle is trustworthy. In addition, in an urban area, there will be no air traffic controller that can be relied on as a common trust anchor. Consequently, the trustworthiness needs to be established peer-to-peer. Consequently, the trust level alone determines the interaction, with physical consequences. For example, it is safer to fly close to a very trustworthy vehicle, while a larger separation needs to be maintained to an untrustworthy one. The mapping of specific challenges of the emergency scenario are given in Table III. In this use case, the system interactions are especially complex. Here, it is especially likely that there is an immediate safety impact, both to people in the air and on the ground.

Table III
EMERGENCY ROADMAP

Challenges	Requirements	Reference
Operation	Hybrid and complex systems	C4.1
Dynamics	Expressive policies	C3.1
	Automatic communication adaptation	A2.2

Consequently, the policies have to be expressive and unambiguous, as time is especially critical in emergency situations. Generally, all vehicles share the responsibility for collision avoidance. Yet vehicles suffering from an in-flight emergency may have limited manoeuvrability and communicability, thus policies need to clearly distinguish between different states so that neighbouring vehicles can efficiently adapt to the new scenario.

Furthermore, if a vehicle suffers from an emergency (or is an emergency vehicle transporting a critically injured patient), the urgency needs to be immediately and automatically communicated to nearby aircraft so that they can make way. This aspect is also intertwined with C2.2 considering temporal metrics, as emergencies are temporary in nature. Hence, a vehicle that claims to have an emergency for a long period of time and does not immediately land at the nearest suitable facility is likely fraudulent and needs to be treated accordingly by other vehicles.

Table IV
FORMATION FLIGHT ROADMAP

Challenges	Requirements	Reference
Data management	Efficient data release	A2.3
	Data trustworthiness	A4.2
Detect	Modelling of the behaviour	C4.4
	Behavioural monitoring	A4.1
React	Dynamic trust adaptation	A1.2
	Contextual Assurance	A4.3

The roadmap for the final use case, formation flight, is given in Table IV. One of the key aspects in this use case is the element of data sharing. Here, it is crucial that data flow is managed efficiently to maximise the benefit of collaboration but also ensuring that the channel is not saturated. However, this is not only a challenge for data security, but also for the overall architectural design. With respect to security, the key element here is ensuring that the data that flows within this (temporary) network is trustworthy and only sent and received by approved members of the formation.

As a flight formation is characterised by a reduced separation between the aircraft, the formation (and with it each individual vehicle) needs to model its own behaviour and that of nearby aircraft. This is intertwined with a close monitoring, to ensure that any divergence between the expected and the actual behaviour is detected as soon as possible. Only this guarantees a timely (and thus safer) reaction to any detected anomaly.

This close proximity also demands that the notion of trust between vehicles is based on their behaviour and adapted dynamically. If one vehicle is found to be no longer trustworthy, the formation needs to quickly break up the formation to gain a safe separation. Moreover, communication links to a compromised vehicle need to be severed immediately to ensure that an infection can not propagate.

VIII. CONCLUSIONS

The safe integration of UASs into a common airspace requires an in-depth solution to secure their interaction with each other and with occupied aircraft. As the systems involved are characterized by a significant heterogeneity with respect to capabilities, certification requirements and automation, such a security solution is far from trivial.

This paper has specifically focused on the notion of trust and the interaction with safety when an interaction or even collaboration is necessary with an untrustworthy vehicle. To this end, three specific interaction use-cases in the challenging scenario of urban air mobility have been presented: collision avoidance, emergency management and formation flight. Four basic requirements for safe UAS interaction and collaboration have been discussed, namely, trust estimation, interaction adaptation, controlled information sharing, and continuous monitoring and assurance. For each of those requirements, the related challenges and actions needed have been given.

Finally, a roadmap has been presented mapping the most significant requirements from the use cases to the identified actions and challenges. This can serve as a basis to better focus future research efforts in the area.

ACKNOWLEDGEMENT

This work has received funding from CONCORDIA, the Cybersecurity Competence Network supported by the European Union's Horizon 2020 Research and Innovation program under grant agreement No 830927.

REFERENCES

[1] P. B. Sujit, D. Kingston, and R. Beard, "Cooperative forest fire monitoring using multiple uavs," in *2007 46th IEEE Conference on Decision and Control*, 2007, pp. 4875–4880.

[2] "Amazon prime air," July 2018. [Online]. Available: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8\&node=8037720011

[3] "Successful trial integration of DHL parcelcopter into logistics chain," July 2016. [Online]. Available: http://www.dhl.com/en/press/releases/releases_2016/all/parcel_ecommerce/successful_trial_integration_dhl_parcelcopter_logistics_chain.html

[4] C. Reiche, C. McGillen, J. Siegel, and F. Brody, "Are we ready to weather urban air mobility (uam)?" in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, 2019, pp. 1–7.

[5] M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "On the security and privacy of ACARS," in *Integrated Communications Navigation and Surveillance (ICNS)*, April 2016, pp. 1–27.

[6] SESAR, "European Drones Outlook Study," https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf, 2016 (acccessed May 19, 2020).

[7] ——, "SESAR's Project Page," https://www.sesarju.eu/U-space, 2020 (accessed May 19, 2020).

[8] SESAR Joint Undertaking, "Supporting Safe and Secure Drone Operations in Europe: A preliminary summary of SESAR U-space research and innovation results (2017-2019)," https://op.europa.eu/en/publication-detail/-/publication/082f56f6-5c3a-11ea-8b81-01aa75ed71a1/language-en/format-PDF/source-120398829, February 2020 (access May 19, 2020).

[9] Civil Aviation Safety Authority, "Civil Aviation Order 20.18," https://www.legislation.gov.au/details/f2013c00121, 2016 (accessed May 19, 2020).

[10] Federal Aviation Administration, "CFR 14 - Aeronautics and Space," https://www.govinfo.gov/app/details/CFR-2017-title14-vol2/CFR-2017-title14-vol2, January 2017 (access May 19, 2020).

[11] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Economy class crypto: Exploring weak cipher usage in avionic communications via acars," in *Financial Cryptography and Data Security*, A. Kiayias, Ed. Springer International Publishing, 2017, pp. 285–301.

[12] D. Bonini, A. Jackson, and N. McDonald, "Do i trust thee? an approach to understanding trust in the domain of air traffic control," in *2001 People in Control. The 2nd International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres*, 2001, pp. 104–109.

[13] http://www.freepik.com.

[14] Y. Mualla, A. Najjar, S. Galland, C. Nicolle, I. Haman Tchappi, A.-U.-H. Yasar, and K. Främling, "Between the megalopolis and the deep blue sky: Challenges of transport with uavs in future smart cities," in *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, 2019, pp. 1649–1653.

[15] European Union Aviation Safety Agency, "Introduction of a regulatory framework for the operation of unmanned aircraft systems in the ópenánd śpecificćategories," https://www.easa.europa.eu/sites/default/files/dfu/Opinion\%20No\%2001-2018.pdf, 2018, [Online; accessed August 2020].

[16] D. D. S. Braga, M. Niemann, B. Hellingrath, and F. B. D. L. Neto, "Survey on computational trust and reputation models," *ACM Comput. Surv.*, vol. 51, no. 5, Nov. 2018. [Online]. Available: https://doi.org/10.1145/3236008

[17] B. Carminati, E. Ferrari, and M. Viviani, *Security and Trust in Online Social Networks*, ser. Synthesis Lectures on Information Security, Privacy, and Trust. Morgan & Claypool Publishers, 2013.

[18] J. Guo, I.-R. Chen, and J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, 10 2016.

[19] I. Ud Din, M. Guizani, B. Kim, S. Hassan, and M. Khurram Khan, "Trust management techniques for the internet of things: A survey," *IEEE Access*, vol. 7, pp. 29 763–29 787, 2019.

[20] Y. Ruan, P. Zhang, L. Alfantoukh, and A. Durresi, "Measurement theory-based trust management framework for online social communities," *ACM Transactions on Internet Technology*, vol. 17, pp. 1–24, 03 2017.

[21] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "Iot passport: A blockchain-based trust framework for collaborative internet-of-things," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, 05 2019, pp. 83–92.

[22] S. Shahrdar, L. Menezes, and M. Nojoumian, "A survey on trust in autonomous systems," in *Intelligent Computing*, 01 2019, pp. 368–386.

[23] F. Mohammed, I. Jawhar, N. Mohamed, and A. Idries, "Towards trusted and efficient uav-based communication," in *2016 IEEE 2nd Conference on BigDataSecurity, on HPSC, and on IDS*, 2016, pp. 388–393.

[24] A. S. Khan, G. Chen, Y. Rahulamathavan, G. Zheng, B. Assadhan, and S. Lambotharan, "Trusted uav network coverage using blockchain, machine learning, and auction mechanisms," *IEEE Access*, vol. 8, pp. 118 219–118 234, 2020.

[25] K. K. Jena, S. K. Bhoi, B. D. Behera, S. Panda, B. Sahu, and R. Sahu, "A trust based false message detection model for multi-unmanned aerial vehicle network," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019, pp. 324–329.

[26] K. Singh and A. K. Verma, "A trust model for effective cooperation in flying ad hoc networks using genetic algorithm," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018, pp. 0491–0495.

[27] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (fanets)," *International Journal of Communication Systems*, vol. 31, no. 6, p. e3517, 2018, e3517 IJCS-16-0655.R2.

[28] E. Ferrari, *Access Control in Data Management Systems*, ser. Synthesis Lectures on Data Management. Morgan and Claypool Publishers, 2010.

[29] E. Bertino, B. Carminati, and E. Ferrari, "Access control for xml documents and data," *Information Security Technical Report*, vol. 9, no. 3, pp. 19–34, 2004.

[30] B. Carminati and E. Ferrari, *Privacy-Aware Access Control in Social Networks: Issues and Solutions*. London: Springer London, 2010, pp. 181–195.

[31] B. Carminati, E. Ferrari, J. Cao, and K. L. Tan, "A framework to enforce access control over data streams," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 3, Jul. 2010.

[32] J. Berger, J. Happe, C. Gagne, and M. Lau, "Co-evolutionary information gathering for a cooperative unmanned aerial vehicle team," in *2009 12th International Conference on Information Fusion*, July 2009, pp. 347–354.

[33] Yan Liao, Yan Jin, A. A. Minai, and M. M. Polycarpou, "Information sharing in cooperative unmanned aerial vehicle teams," in *Proceedings of the 44th IEEE Conference on Decision and Control*, Dec 2005, pp. 90–95.

[34] C. Ardagna, R. Asal, E. Damiani, T. Dimitrakos, N. El Ioini, and C. Pahl, "Certification-based cloud adaptation," *IEEE TSC*, 2018.

[35] C. Ardagna, R. Asal, E. Damiani, and Q. Vu, "From security to assurance in the cloud: A survey," *ACM CSUR*, vol. 48, no. 1, pp. 2:1–2:50, August 2015.

[36] M. Anisetti, C. Ardagna, N. Bena, and E. Damiani, "Stay thrifty, stay secure: A vpn-based assurance framework for hybrid systems," in *Proc. of the 17th International Conference on Security and Cryptography (SECRYPT 2020)*, online, July 2020.

[37] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust, a security assessment model for infrastructure as a service (iaas) clouds," *IEEE TCC*, vol. 5, no. 3, pp. 523–536, July 2017.

[38] C. Ardagna, E. Damiani, J. Schutte, and P. Stephanow, "A case for IoT security assurance," in *Internet of Everything*, B. D. Martino, K. C. Li, L. Yang, and A. Esposito, Eds. Springer, 2017.

[39] H. Sato, A. Kanai, S. Tanimoto, and T. Kobayashi, "Establishing trust in the emerging era of iot," in *Proc. of IEEE SOSE 2016*, Oxford, UK, March–April 2016.

[40] S. Taherizadeh, A. Jones, I. Taylor, Z. Zhao, and V. Stankovski, "Monitoring self-adaptive applications within edge computing frameworks: A state-of-the-art review," *Journal of Systems and Software*, vol. 136, pp. 19–38, 2018.

[41] C. Ardagna, R. Asal, E. Damiani, N. El Ioini, and C. Pahl, "Trustworthy iot: An evidence collection approach based on smart contracts," in *Proc. of the 15th IEEE International Conference on Services Computing (SCC 2019)*, Milan, Italy, July 2019.

[42] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, November 2016.

[43] C. G. L. Krishna and R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Proc. of the 15th IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR 2017)*, Shanghai, China, October 2017.

[44] M. Morovitz, "Security Vulnerabilities in Unmanned Aircraft Systems," http://www.cs.tufts.edu/comp/116/archive/fall2015/mmorovitz.pdf, 2015.