symmetry

MDPI

Article

Study on Destructive Informational Impact in Unmanned Aerial Vehicles Intergroup Communication

Egor Marinenkov [1,*], Sergei Chuprov [2,3,*], Nikita Tursukov [2], Iuliia Kim [2] and Ilia Viksnin [2,*]

[1] Network Technologies Office, ITMO University, 197101 Saint Petersburg, Russia
[2] Mobile Intelligent Systems Laboratory, ETU "LETI" University, 197022 Saint Petersburg, Russia; stepingnik@gmail.com (N.T.); yulia1344@gmail.com (I.K.)
[3] Golisano College of Computing and Information Sciences, Rochester Institute of Technology, Rochester, NY 14623, USA
* Correspondence: egormarinenkov@gmail.com (E.M.); sc1723@rit.edu (S.C.); wixnin@mail.ru (I.V.)

Abstract: In this paper, we propose a novel approach to formalize the impact of malicious intergroup informational attacks toward a group of unmanned aerial vehicles communication. Infrequent but critical situations arise when an already authorized group member starts to transmit false data to other group participants. These scenarios can be caused by a software or hardware malfunction or a malicious attack, and cannot be prevented by the conventional security measures. The impact of such actions can be critical for a group's performance. To address this issue, we develop and formalize the model of unmanned aerial vehicles' intergroup communication and provide the calculus for a group's performance destructive impact. We employ a multi-agent-based approach to formalize the information interaction between the participants of the unmanned aerial vehicles group. The model we propose possesses such properties as symmetry and scalability, as it considers individual participants as separate homogeneous distributed agents that have to perform their tasks in parallel to achieve the joint group goal. We classify informational threats by the type of the destructive impact they cause: apparent and hidden. Data contained in informational messages is categorized according to the agent's destructive impact premeditation degree: intentional and unintentional. To verify the model proposed, we conduct an empirical study. The results show that the false data transmitted during the intergroup communication adversely affects the group's performance, and such an impact can be measured and quantified.

Keywords: unmanned aerial vehicle; security; safety; hidden destructive impact

Citation: Marinenkov, E.; Chuprov, S.; Tursukov, N.; Kim, I.; Viksnin, I. Study on Destructive Informational Impact in Unmanned Aerial Vehicles Intergroup Communication. *Symmetry* **2022**, *14*, 1580. https://doi.org/10.3390/sym14081580

Academic Editors: Kholod Ivan, Alexey Paznikov and Vasily Desnitsky

Received: 29 June 2022
Accepted: 27 July 2022
Published: 1 August 2022

1. Introduction

The rapid evolution of information technology has considerably altered all areas of human activities. Progress and advances in the field of robotics and transport have led to the emergence of unmanned aerial vehicles (UAVs), which have basically become known as drones. There is a number of possible tasks for an individual aerial vehicle to perform. However, grouping UAVs to solve one common collective task can be more effective in some situations. UAV groups have also become known as "swarms" [1], as their group behavior organization is similar to miscellaneous living organisms. A swarm of UAVs possesses properties of a self-organizing system, which contains interacting elements and is able to perform tasks due to this interaction [2–5]. Such advantages as scalability, efficiency, and reliability in task performance can be achieved with the application of UAV intergroup communication.

UAVs intergroup communication is vulnerable to various security threats. Exploiting vulnerabilities may substantially decrease the efficiency of the group performance, which may result in fails or a system's complete outage. Security and safety assurance of informational messages, which are transmitted between group participants, are vital to ensure

correct operation and goals achievement. Thus, proper and safe group operation requires identifying threats and vulnerabilities and implementing valid countermeasures.

Attacks toward the security of communication in Internet of Drones have been actively investigated in the literature for the last decade [6–8]. However, current research usually concentrates only on "conventional" attacks against data communication, such as eavesdropping, man-in-the-middle, jamming, and other attacks, which are intentionally initiated by an attacker. Such attacks commonly can be detected or mitigated by the appropriate defense mechanisms [6]. In contrast to this approach, we address another type of so-called "soft" attacks [9], which remain to be under-researched. These attacks can be provided intentionally or inadvertently by a failed or maliciously attacked UAV. For instance, a UAV can transmit false data on its current location to other group participants due to sensor system failure. In this case, the attack cannot be detected or mitigated only with conventional defense mechanisms, as the structure, integrity, and other patterns of the transmitted message are not maliciously modified. However, the data transmitted by this message is false, as it does not reflect the real UAV's location.

In this paper, we follow the approach to consider the group of UAVs as agents of a multi-agent system, which have to interact with each other and perform local tasks to achieve a global goal under dynamic environmental conditions [10,11]. In such a type of system, agents need to communicate and coordinate their movements with each other to optimize the resource consumption and avoid collisions. Collision avoidance in a group of multiple UAVs is not a trivial task and requires applying special techniques, as it is necessary to deal with it both on individual and group levels [12]. False data, provided to other group participants by a failed or maliciously attacked UAV, may lead to various unpleasant consequences, from sub-optimal resource consumption and task allocation to collision with other UAVs or surrounding objects. Considering that groups of UAVs are primarily utilized in real-time applications and hostile dynamic environments (e.g., wide-area monitoring, and rescue operations), the provision of false data by one or several UAVs may be damaging for a UAV group's user in various contexts. Generally, a hostile environment increases the threats likelihood for a UAV intergroup communication [13]. However, as practice has shown, security and safety are not commonly addressed at the various stages of a robotic system design life cycle [9]. Multigroup UAVs are usually based on resource-constraint hardware platforms, which allow to make individual drones cheap, lightweight, and reliable, but unable to utilize complex defense mechanisms that require substantial computational performance.

The issues mentioned above raise the need to establish the relationships between the provision of false or incorrect data by a UAV to other group participants and the effect it has on the overall group performance. The effect from providing false data can vary depending on the UAV and situation, and can cause different damages. The investigation and quantification of this damage can help users to evaluate their risks while employing a group of UAVs for their tasks, and can help the UAVs developers and researchers to better plan the security and safety measures that they need to implement.

In the present work, we explore the interrelations between the false data provided in the process of the UAV intergroup communication and the performance of the UAV group. Through the intergroup communication mechanism, group participants can interact and decide which of them affect the whole group's performance via the destructive informational impact (DII). Under DII, we understand the impact, which can be detected by other participants and decreases the performance of individual participants or the whole UAV group. Moreover, we examine the hidden destructive informational impact (HDII), which is understood as an impact that cannot be detected using UAV sensors and conventional security methods, and which decreases the system's performance [9,14–17].

The contribution of this research is twofold. First, we provide the calculus to evaluate and quantify DII and HDII in the UAV intergroup communication. In our approach, we follow multi-agent system principles [18] and represent each UAV as individual agent with the uniform features. The agents have to perform their tasks in parallel to achieve

the common group goal. During their operation, agents have to build optimal routes and reconfigure them in case of collision avoidance. This distributed system organization manner introduces scalability and symmetry into the model we employ. In addition, agents are able to communicate with each other and plan their optimal routes based on the data on the environment, provided by other group participants. We also systematize types of DII and develop a taxonomy of HDII based on the adversarial intention degree.

Second, we conduct an empirical study, in which we model destructive informational impacts and analyze their consequences on a UAV group performance. We assume our calculus and the results can be beneficial for the community both to improve the conventional security and safety methods and to develop novel ones.

The paper is organized as follows. Section 2 briefly reviews the research, which proposes both conventional security and safety methods, and approaches based on decentralized UAV group management. Section 3 describes our model of intergroup communication. Section 4 reveals informational interaction vulnerabilities and classifies them into internal and external ones. Threats description, damage types taxonomy and calculus are proposed in Section 5. Section 6 contains the approach validation, simulation setup description, and interpretation and analysis of the results obtained. Section 7 provides conclusions and introduces further research points.

2. Related Work

Vulnerabilities arising in the process of intergroup communication have actively been investigated in the literature [19–22]. It should be emphasized that in the case of central control device (CCD) presence, the interaction between group participants and CCD is considered. Approaches and methods to secure the communication channel from such attacks as spoofing, jamming, DDoS, etc., are analyzed. Centralized and decentralized group management strategies are considered, with the opportunity of using UAVs groups for both civilian and military purposes.

Watkins et al. [23] demonstrate an example of communication channel organization between UAVs group participants and CCD, which allows remote wireless connections. Hard-to-patch vulnerabilities and back doors in popular models of drones are used to implement malicious attacks. Applying this approach, it is possible to use a laptop or Android OS smartphone for identifying, tracking and executing some control commands on rogue UAVs.

In [24–26], a multi-agent approach is employed to analyze the UAV group as a self-organizing system. In these papers, the authors consider the organization of decentralized actions between group participants. However, for remote control purposes and actions coordination, CCDs are used. In their research, the authors jointly conclude that it is necessary to organize secure information interaction between the group participants, taking into account known attacks and analyzing possible vulnerabilities related to intergroup communication.

Refs. [19–26] provide a fresh look at various vulnerabilities, related to UAVs intergroup interactions. They show that the conventional security methods are ineffective against attacks, aimed at informational messages context falsification. The models and methods described are based on the decentralized group management strategy and can be applied to counter different attacks.

In our paper, in contrast to considering only apparent DII, we focus on investigating the HDII both on the overall group and on single group participants. Therefore, our aim is to analyze the effects of HDII in the process of UAV intergroup communication on the group's performance. To achieve this aim, we determine the following tasks:

- Define and formalize the UAVs intergroup communication process;
- Define DII and HDII and develop calculus for their evaluation;
- Analyze the effects of HDII;
- Validate the HDII negative effects on the group's performance via an empirical study.

To assess the UAV group's performance in the empirical study, we evaluate the number of completed tasks by the group participants. Deviations of this number from the "ideal" case, without any DII or HDII in the process of intergroup communication, are used to assess the negative impact provided.

3. Model of Intergroup Communication

To represent UAVs intergroup communication, we propose a theoretical model, based on the decentralized management strategy. In [27], the types of group management strategies are described in detail. To identify an appropriate strategy for the present research, we analyzed these strategies [28]. In terms of safety and security assurance, the decentralized strategy is more relevant, as there is no CCD that can be treated as a single point of failure. Therefore, computational workload on each group participant is far less than with the centralized strategy, and the decision-making process is less time consuming. In addition, the communication channel presence between group participants allows to organize tasks allocation using dynamic task auctions [29].

We propose to divide the informational interaction (II) between group participants into two types: external and internal. Internal II relates to the individual group participant and is represented by the communication between various computing devices and sensors collecting environmental information. Each UAV has a processing unit (PU), which processes gathered information and generates control commands. Thus, internal II refers to the data on the current UAV coordinates, position in space, angles of inclination, technical condition, control movement commands and tasks, that circulates among computing devices, sensors and PU.

Communication between two or more UAVs relates to the intergroup communication and is considered external II. Such informational messages may include the UAV localization data, location of obstacles, its technical condition, and other information, relevant for tasks performance. Based on this data, UAV group is able to allocate tasks among agents and perform them.

As an assumption, we consider only an ideal communication channel conditions, which means the absence of any interference and packet losses in the communication process [30]. Our model assumes that UAVs group participants communicate and aspire to achieve a collective goal. Let us formulate this goal. The main goal of the UAVs group is to perform a maximum number of tasks at minimum costs. Let $U = \{u_1, \ldots, u_n\}$, where u_i is i-th UAV, $T = \{t_1, \ldots, t_m\}$, where t_j is a j-th task, assigned to the group. Let C be the tasks cost matrix (1), where $cost(u_i, t_j)$ is a function for calculating the cost of performing the task t_j by the u_i UAV.

$$C = \begin{pmatrix} c_{11} & \ldots & c_{1m} \\ \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nm} \end{pmatrix}, c_{ij} = cost(u_i, t_j) \tag{1}$$

Let us consider that UAVs perform some tasks throughout the entire functioning life cycle, then $T^d \subseteq T$, where T^d is a set of the completed tasks. Then $T^d = \bigcup_{i=1}^{n} T_i^d, T_i^d \cap T_k^d = \varnothing, T_i^d = \{\ldots, t_j^i, \ldots\}$, where T_i^d and T_k^d are sets of completed tasks by u_i and u_k UAVs respectively, t_j^i is a task, completed by u_i UAV.

Let r_i be the UAV u_i energy resource, then the group goal can be expressed through the optimization task, represented by (2).

$$\begin{cases} |T^d| \to |T| \\ \sum_{i=1}^{n} \sum_{j=1}^{m} cost(u_i, t_j^i) \to 0 \\ \sum_{j=1}^{m} cost(u_i, t_j^i) < r_i \end{cases} \tag{2}$$

These are the conditions to achieve the functioning general task for the UAV group. However, in the case of any malicious attacks on intergroup communication, the group goal might not be achieved, which would mean the destructive impact application.

The process of performing a particular task by a group can be divided into two stages: task allocation auction, and task execution. The aim of the auction is to identify the most appropriate performer among the entire group for the particular task [27]. To participate in the auction, the UAV must participate in the intergroup communication and have no any technical defects. To be selected as the task executor, UAV should have enough resources to perform this task. Task execution starts from the moment the tasks are allocated until the particular task completion. Prior to the task completion, UAV exchanges its current location and environmental conditions data with the other group participants.

The following points are important for the UAVs group in the process of tasks performance: communication possibility, technical state, energy resource, localization and environmental conditions data. Within the proposed model, technical state and energy resource are internal factors, localization and environmental data refer to external functioning factors. Communication is a crucial factor for intergroup communication and group goal achievement.

As a part of the collective management strategy, all UAVs participate in the auction on each iteration of the functioning time. Completion of the tasks allows the group to achieve the goal. It can be reached by the following rules:

- If u_i have no technical issues, it participates in the task allocation auction;
- If u_i is not performing the task now, it participates in the task allocation auction;
- If $cost(u_i, t_j^i) < r_i$, u_i participates in the task allocation auction for t_i;
- If $cost(u_i, t_j^i) < cost(u_k, t_j^k)$, where $k \neq i$, t_j is assigned to u_i.

The task is assigned to the UAV only in the case that it corresponds to all the conditions, set by the rules listed above. The task allocation auction is schematically represented in Figure 1. It incorporates several steps, the aim of which is to allocate the task to the most suitable UAV in terms of the distance, current resource balance, and technical condition. The auction's steps are described in more detail below.

1. The first step incorporates the appropriate technical state check. Particular technical checks may vary on a specific UAV's characteristics and user or application requirements. For example, it may be a software integrity test or a hardware operation mode check.
2. The aim of the second step is to verify if the UAV already assigned a task to perform. In the UAVs' group initialization moment, all the UAVs have "free" status. Then, after the task is allocated to a specific UAV, its status changes to "busy".
3. The third step incorporates the resource balance check. The UAV's approximate resource consumption to perform the task is calculated according to the distance to the task and UAV's characteristics, which can vary depending on the user or application requirements. If the UAV has enough resources to perform the task, it proceeds to the next step of the auction.
4. The fourth step's aim is related to the evaluation of the distance between the task location and the UAV. The UAV that is closest to the task's location is selected to perform it, if it passes the resource balance check.
5. On the fifth step, the UAV changes its status to "busy" and starts to perform the task.
6. After the task is performed, the UAV changes its status to "free", and participates in the task allocation auction again. If there are no tasks to allocate, the UAV stands by and waits for the next tasks to be allocated.

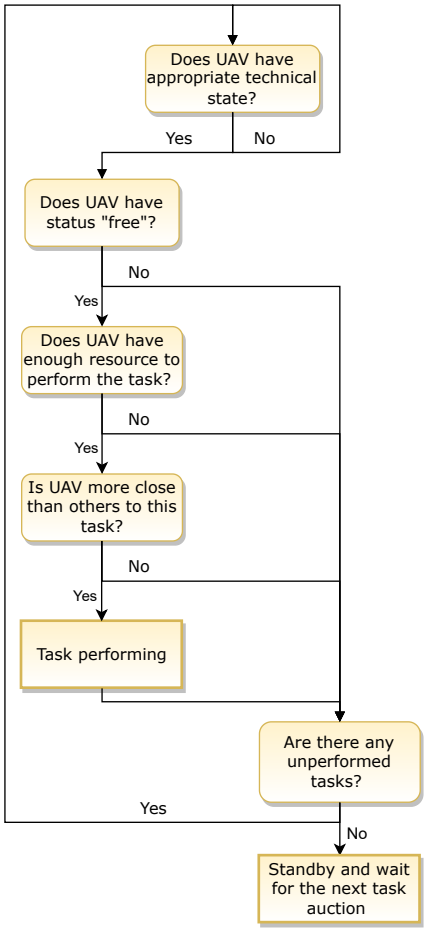

Figure 1. Task allocation auction steps diagram.

4. Informational Interaction Vulnerabilities

4.1. UAV Internal Informational Interaction Vulnerabilities

Based on the II classification and description, an issue on vulnerable UAV devices and sensors for environmental data gathering and processing is raised. Environmental scanning and localization devices gather and process data on the surroundings. This data can be falsified by a malicious UAV or a third party. Thus, such devices are vulnerable to DII. After the environmental data collecting procedure, the devices process and transmit this data to the PU, which means that PU is vulnerable to DII from scanning and localization devices. Moreover, it is necessary to consider that space movement, and other additional devices are further vulnerable to DII from the PU.

Considering the internal II in the UAV as a chain of information flow (Figure 2), it can be supposed that space-movement control components and additional devices are the most vulnerable to DII, because they are located at the end of this chain. Therefore, in the case of DII on the previous components in the chain, further modules gather and process falsified data, which is likely to significantly affect the UAV group's performance. Figure 3 represents the concept of UAV internal II between the UAV system components. In this paper, we represent UAV as a system, which integrates the following components:

- Environmental sensors, which are devices designated to obtain the measurements from the environment. Particular devices can vary depending on the UAV's characteristics and user or application requirements. Example of such devices are on-board cameras, ultrasonic range finders, LiDARs, etc.
- Localization devices, which are devices designated to perform localization and mapping of the UAV. Examples of such devices may be a GPS or a GLONASS sensors.

- Processing unit, which is the main computational core of the UAV. We assume that this component incorporates all the software and hardware that UAV uses to perform its computational tasks, such as decision making, processing of the received data, distance to obstacle evaluation, etc.
- Movement adjustment devices that incorporate rotors, blades, and devices to control them. These devices are used to adjust movement, regulate altitude, and control flight direction and speed.
- Task execution devices may include any devices that are required to perform a specific task. They may vary depending on the user or application requirements, an example may be a capturing device designated to transport cargo.

Bold arrows in Figure 3 indicate information flows vulnerable to DII. Thereafter, if HDII applied, the informational messages containing data on the technical state and energy resource can be falsified.

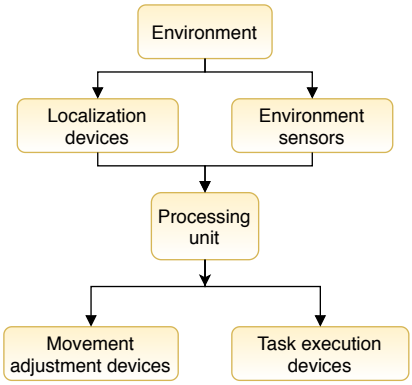

Figure 2. Direction of II flows between UAV components, represented as a chain.

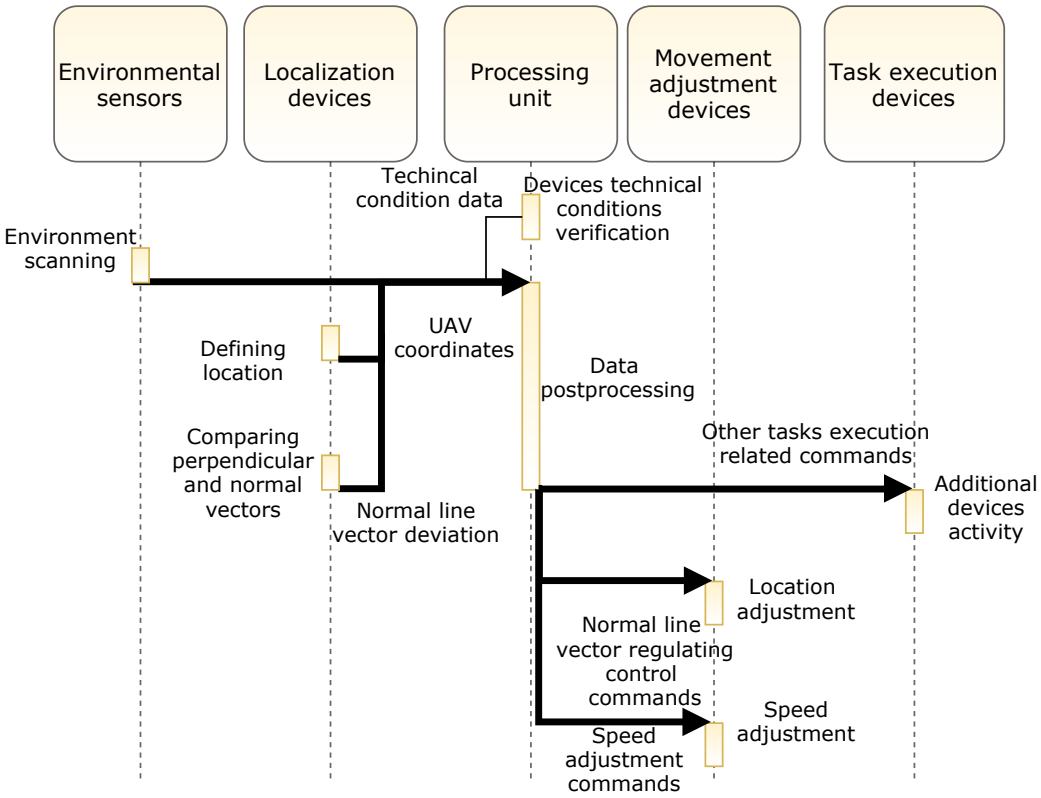

Figure 3. Detailed schematic representation of the environmental data gathering and processing by UAV components. Highlighted arrows indicate information threads vulnerable to DII.

4.2. UAVs External Information Interaction Vulnerabilities

The UAVs group consists of n participants and transmits information to each other, based on which further decisions are made. For the research purposes, let us introduce an assumption of i-th UAV faultless, so that the UAV cannot be a source of falsified data.

The informational messages received by the i-th UAV from the particular UAV and the data broadcast during intergroup communication are vulnerable to DII. While in the former case, informational messages are transmitted directly from one UAV to another, in the latter one, the data is broadcasted and processed by all group participants.

5. Threats Classification

As described in [16,31–39], conventional security methods can detect the apparent DII and are applicable to the UAVs group. Hereupon, the following HDII types can be considered.

HDII can be classified as intentional or unintentional. In Figure 4, we schematically represent the classification of the HDII types by a vulnerable component from which HDII originates from. The intentional impact is implemented to decrease the UAV group performance by a malicious UAV or a third party. The unintentional one occurs in cases of technical faults in the UAV's hardware or software components. Connection type factors, internal and external factors can be used to identify the HDII type.

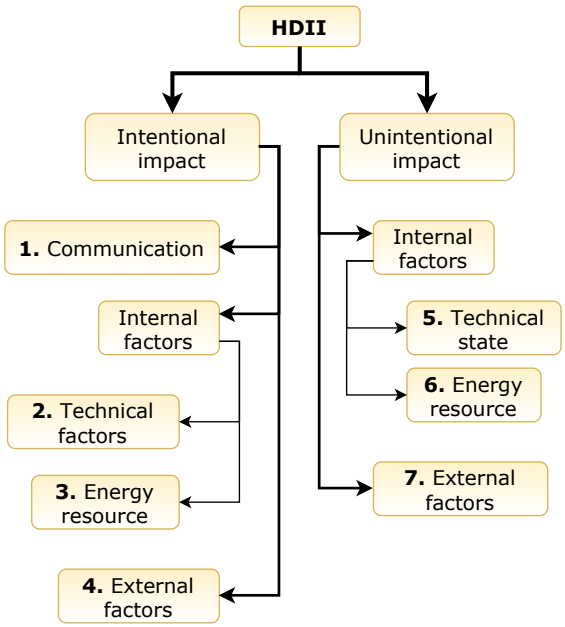

Figure 4. HDII classification by a vulnerable component in UAVs intergroup communication.

To describe the consequences of HDII, we introduce the T^d_{HDII} indicator, which is a set of completed tasks in the case of HDII implementation, k is a number of UAVs, providing given HDII, and $cost_{HDII}(u_i, t_j)$ is a function calculating the task cost during HDII implementation.

Each HDII type can lead to different consequences:

- Direct damage. In this type of damage, the number of completed tasks is affected directly, defined by (3).

$$|T^d| > |T^d_{HDII}|; \tag{3}$$

- Undefined type of damage. The threat of UAVs group participants violation (in the case when the agent takes the task and spends energy in the process of its implementation) is represented by (4).

$$c_{ik} < r_i - \sum_{j=1}^{m} cost(u_i, t_j^i), k \neq j; \tag{4}$$

- Indirect damage. Increase in the average costs of performing the task by an individual group participants leads to the growth of the overall group costs. This type of damage is defined by (5).

$$\begin{bmatrix} \sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i, t_j^i) < \sum_{i=1}^{n}\sum_{j=1}^{m} cost_{HDII}(u_i, t_j^i) \\ \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i, t_j^i)}{T^d} < \frac{\sum_{i=1}^{n-k}\sum_{j=1}^{m} cost(u_i, t_j^i)}{T^d_{HDII}} \end{bmatrix}. \tag{5}$$

Below, we present a more rigorous HDII classification with a scenario description and effect evaluation.

1. UAV does not participate in II and in the task allocation auction, but has such an opportunity.
   (a) Indirect damage. Average task costs of individual participants may increase with a constant number of completed tasks, defined by (6).

$$\begin{cases} \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d} < \frac{\sum_{i=1}^{n-k}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d_{HDII}} \\ |T^d| = |T^d_{HDII}| \end{cases} \tag{6}$$

   (b) Direct damage. A number of completed tasks may decrease with the constant costs for performing these tasks. This type of damage is defined by (7).

$$\begin{cases} \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d} = \frac{\sum_{i=1}^{n-k}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d_{HDII}} \\ |T^d| > |T^d_{HDII}| \end{cases} \tag{7}$$

2. UAV provides false data on its technical state and does not participate in the task allocation auction.
   (a) Indirect damage. The average UAV individual task costs may increase with the constant number of completed tasks. This type of damage is defined by (8).

$$\begin{cases} \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d} < \frac{\sum_{i=1}^{n-k}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d_{HDII}} \\ |T^d| = |T^d_{HDII}| \end{cases} \tag{8}$$

   (b) Direct damage. The number of completed tasks may decrease with the constant number of standard costs. This type of damage is defined according to (9).

$$\begin{cases} \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d} = \frac{\sum_{i=1}^{n-k}\sum_{j=1}^{m} cost(u_i,t_j^i)}{T^d_{HDII}} \\ |T^d| > |T^d_{HDII}| \end{cases} \tag{9}$$

3. Direct damage. UAV provides false data on the lack of energy resources to perform tasks. In this case, the number of UAVs participating in the task allocation auction does not decrease. Such a scenario can lead to task completion failure due to an

increase in costs of particular UAVs. As a consequence, other group participants are unable to take this task: $|T^d| > |T^d_{HDII}|$.

4. UAV provides false data on its location or environmental conditions.
   (a) Indirect damage. This type of behavior can lead to a task cost deviation, illustrated by (10).

$$\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i, t^i_j) < \sum_{i=1}^{n}\sum_{j=1}^{m} cost_{HDII}(u_i, t^i_j) \tag{10}$$

   (b) Undetermined damage. UAV may face a lack of energy resources during the task performance. This can be a result of sub-optimal route selection. It is defined according to (11).

$$c_{ik} < r_i - \sum_{j=1}^{m} cost(u_i, t^i_j), \text{where } k \neq j \tag{11}$$

   (c) Direct damage. As a result, the above-described consequences convergence can lead to a decrease in the number of tasks completed: $|T^d| > |T^d_{HDII}|$.
5. Direct damage. UAV provides false data on its appropriate technical state. Thus, the task can be assigned to the UAV, but it is unable to perform this task. Therefore, $|T^d| > |T^d_{HDII}|$.
6. UAV provides false data on its energy resource.
   (a) Undetermined damage. In this case, implemented HDII results in UAV battery discharge before it completes the task. Defined by (12).

$$c_{ik} < r_i - \sum_{j=1}^{m} cost(u_i, t^i_j), \text{where } k \neq j \tag{12}$$

   (b) Direct damage. In such a scenario, implemented HDII may lead to a decrease in the completed tasks number: $|T^d| > |T^d_{HDII}|$.
7. UAV transmits false localization or environmental conditions data.
   (a) Indirect damage. This type of behavior can affect the number of tasks completed. It is defined according to (13).

$$\sum_{i=1}^{n}\sum_{j=1}^{m} cost(u_i, t^i_j) < \sum_{i=1}^{n}\sum_{j=1}^{m} cost_{HDII}(u_i, t^i_j) \tag{13}$$

   (b) Undetermined damage. Other group participants may face a lack of energy resources during tasks performance. This can be a result of sub-optimal route selection. It is defined by (14).

$$c_{ik} < r_i - \sum_{j=1}^{m} cost(u_i, t^i_j), \text{where } k \neq j \tag{14}$$

   (c) Direct damage. Increasing of tasks costs or UAVs failures may affect the overall group performance: $|T^d| > |T^d_{HDII}|$.

For better visualization, the described types of damage are structured in Table 1. The situations described naturally lead to the deviations in the UAVs group performance, compared with the "ideal" case, without any destructive impact. In particular, the application of such impacts can affect both the individual and the overall UAV group performance. Thus, developing and implementing safety and security methods that can counter these attacks is of paramount importance.

Table 1. HDII damage types taxonomy.

Direct	Undetermined	Indirect
The agent does not participate in the II and, as a consequence, in the auction, but has such an opportunity (1b, according to Section 5)	The agent provides false localization and environmental data (4b, according to Section 5)	The agent does not participate in II and, as a consequence, in the auction, but has such an opportunity (1a, according to Section 5)
The agent provides false data on the technical state and does not participate in the auction (2b, according to Section 5)		The agent provides false data on the technical state and does not participate in the auction (2a, according to Section 5)
The agent provides false data on the remaining resources to perform tasks (3, according to Section 5)	The agent believes that has enough energy resources to perform the task (6a, according to Section 5)	
The agent provides false localization and environmental data (4c, according to Section 5)		The agent provides false localization and environmental data (4a, according to Section 5)
The agent believes that it has a proper technical state (5, according to Section 5)	The agent reports incorrect localization and environmental data (7b, according to Section 5)	
The agent believes that it has enough energy to perform the task (6b, according to Section 5)		The agent reports false localization and environmental data (7a, according to Section 5)
The agent reports incorrect localization and environmental data (7c, according to Section 5)		

6. Empirical Study of HDII Effect on UAVs Group Performance

To achieve the research aim we established, we conduct an empirical study on HDII in UAVs intergroup communications. To model the group of UAV and the communication between its participants, we leveraged the CoppeliaSim robotic simulation environment. To accomplish the task throughout the modeling process, UAVs are supposed to move through a narrow corridor surrounded by the walls created on a simulation map. For UAVs, it is necessary to detect the obstacles (walls), since these obstacles cross the shortest trajectory from the UAV start to the finish point. The example of the UAV's logic for obstacles overcoming is given below as the simplified pseudo-code Algorithm 1.

Algorithm 1: Example of obstacles overcoming algorithm employed in the empirical study.

```
Result: Chosen moving direction
initialization;
if the obstacle is in front then
    if the obstacle is not on the right then
        take 10 degrees right;
    end
    if the obstacle is not on the left then
        take 10 degrees left;
    end
else
    move forward;
end
```

In the case of UAV's sensor malfunction during the process of environmental data gathering, proper obstacle position detection can fail. Therefore, this negative effect relates to DII. For the illustration purposes, we outline the key moments of the empirical study: corridor entry (Figure 5); collision with an obstacle due to the DII caused by the ultrasonic range finder, which results in improper command generation by the PU (Figure 6); UAV crash, caused by the destructive impact on the system components (Figure 7).

To evaluate the DII effect on the UAV's group performance, we empower one of the UAV to provide DII on other "harmless" group participants. As a result, one of the "harmless" UAVs crashed. Such an impact could not be identified as destructive by the other group participants, and therefore could not be neutralized or mitigated by the employed security and safety measures. This allows us to consider the caused impact as HDII, which affects the context of broadcasting informational messages.

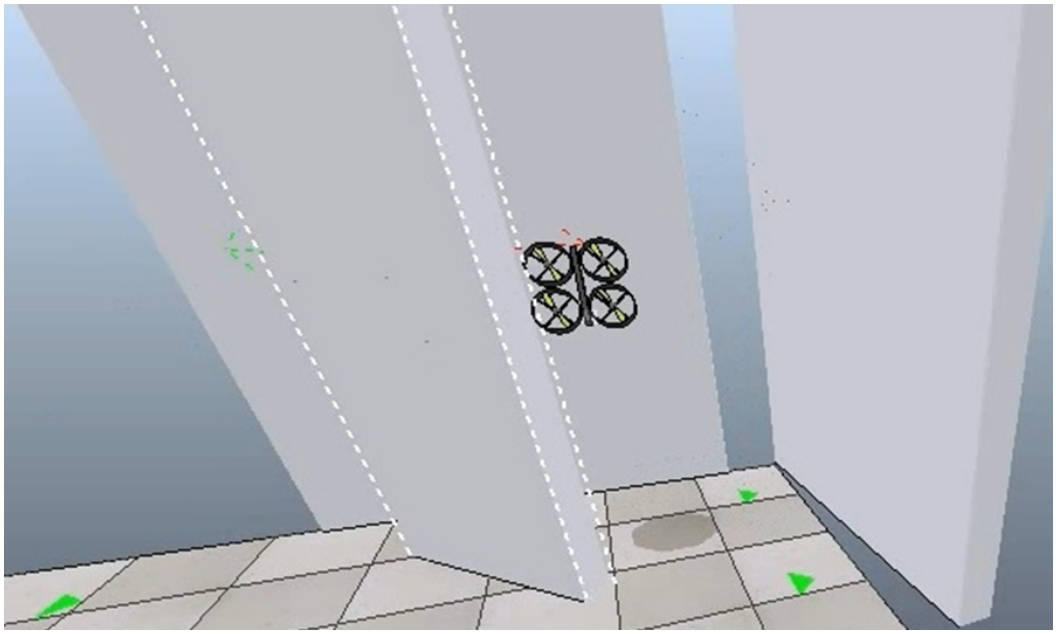

Figure 5. The experiment's initialization moment. Entry into the corridor with obstacles. The green triangles on the floor represent the tasks' location. The green and red arrows on the sides of the wall are simulator's built-in functions that represent to which directions the wall can be moved.

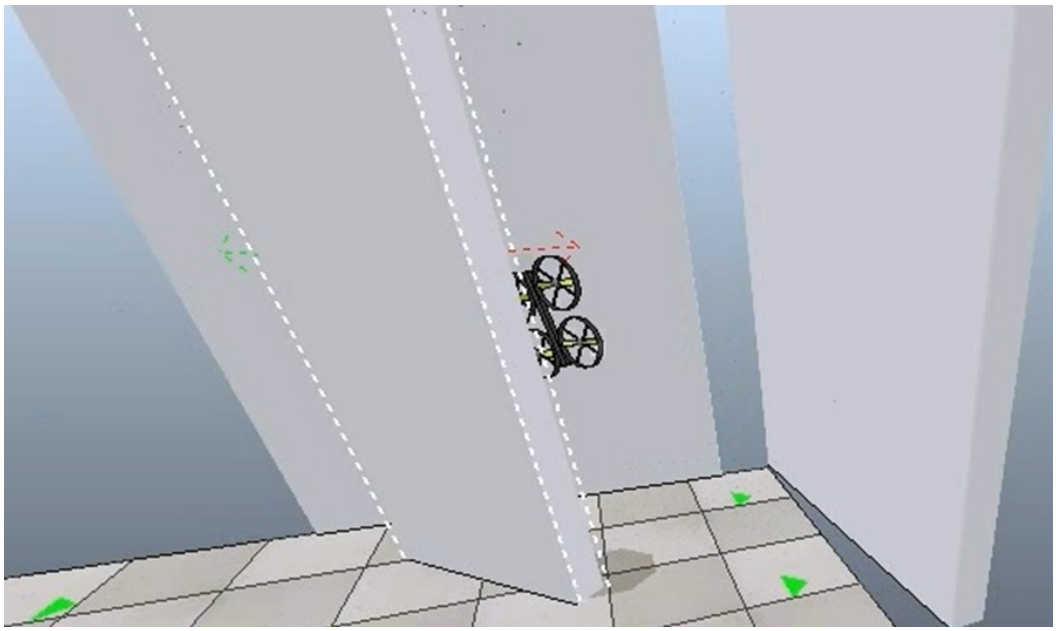

Figure 6. The moment of UAV's collision with the obstacle. The green triangles on the floor represent the tasks' location. The green and red arrows on the sides of the wall are simulator's built-in functions that represent to which directions the wall can be moved.

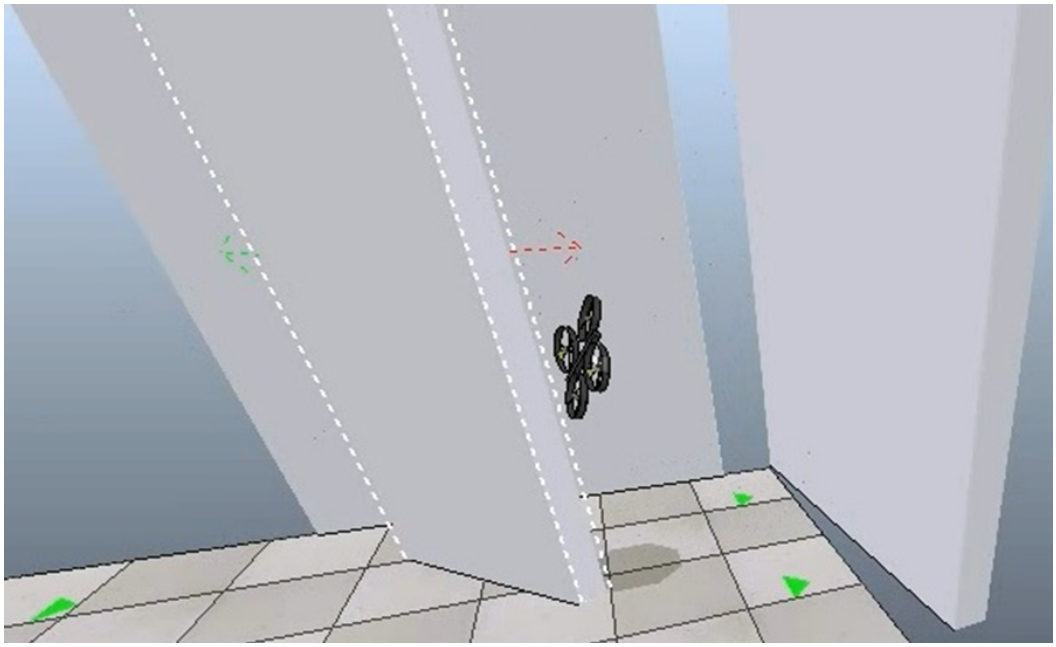

Figure 7. The moment of UAV's crash, caused by the destructive impact on its system components. The green triangles on the floor represent the tasks' location. The green and red arrows on the sides of the wall are simulator's built-in functions that represent to which directions the wall can be moved.

6.1. Simulation Setup

The simulation testbed can be described as a finite cube with a discrete size of $10 \times 10 \times 10$ elementary space blocks (ESBs). The particular block size depends on the size the particular UAV and its individual space. The size of the individual UAV is $0.3 \times 0.3 \times 0.15$ m, and its individual space is a sphere with a UAV in its center, where the sphere diameter D is the parallelepiped with a diagonal $D = \sqrt{0.3^2 + 0.3^2 + 0.15^2} = 0.792$ m. We assume that ESB is a cube with a sphere of diameter D inscribed in it. Then, the side of the cube can be defined as $a = D = 0.792$ m. In addition, the ESB dimensions are rounded: $a = 0.8$ m. Therefore, the actual size of the ESB is $0.8 \times 0.8 \times 0.8$ m.

The UAVs group consists of five participants. In the initialization moment, they are located in zone A, painted turquoise in Figure 8. The aim of each UAV is to reach the finish point, where the "flag" is located (represented as green triangles in Figures 8–10) and to return to the zone A in the most optimal way (in terms of distance). The goal of the whole group is to perform 10 abstract tasks (to reach the "flag" and return to the zone A).

In the initialization moment, a unique identification number (ID) is assigned to each UAV. Each of the participants is located on their own certain ESB, from which they start moving toward the target. Further, tasks are allocated among the participants via the auction. Tasks are distributed according to the minimum distance rule, that is, the task is assigned to the agent closest to the target and not occupied by another task. Each task has its own unique ID number (from 1 to 10) and a certain status:

- Unperformed, if the task has not been assigned to any of the UAVs yet;
- In progress, if the task is assigned to one of the UAVs, but has not been completed yet;
- Completed, if the task has been completed.

Once the UAV with the assigned task reaches the "flag" and transports it to zone A, the task status can be defined as "completed", and the UAV status as "free". The UAV's status can have the following values:

- "Free", if the UAV is not performing any task at the current moment;
- "Unavailable", if the UAV is in the process of task performing.

After all tasks are defined as "completed", the overall group's goal is considered achieved. To avoid collisions and conflicts in the movement control process, the following assumptions are introduced:

- If the distance towards the "flag" from two or more UAVs is equal, the task is assigned to the participant with a highest ID;
- If the distance towards two or more tasks from the UAV is equal, the task with the minimal ID is assigned to the UAV;
- If there are no tasks with the "unperformed" status, the UAV stays in the zone A.

Let us formalize the UAV group activities for our empirical study. There is a set $A = \{a_1, \ldots, a_5\}$, where a_i is the ESB of the i-th, $i = \{1, 2, 3, 4, 5\}$ UAV starting point. The set $t = \{t_1, \ldots, t_{10}\}$, where t_j is the ESB of the j-th "flag". We assume that each UAV performs at least one task, then for each UAV, the functioning process can be divided into N stages, where $1 \leq N \leq 6$ (the maximum number of stages is defined based on the following scenario: all UAVs, except one, have completed one task, thus the remaining task-unassigned UAV is forced to perform the remaining five tasks). The task is assigned to i-th UAV if the finish point distance is minimal, according to (15).

$$P_{ij} = min(\rho(a_i, t_j)), \tag{15}$$

where P_{ij} is the optimal possible path toward the flag, and ρ is the distance between a_i and t_j.

For our particular simulations, we assume the remaining unperformed tasks as a consequence of DII provided by one of the UAVs. Moreover, such a UAV can also provide HDII by transmitting false data to other group participants. Such informational messages cannot be identified as falsified ones by other group participants, which leads to sub-optimal decisions. Furthermore, such false data results in the group tasks' performance decrease, which can be demonstrated by our experiments. The inability of UAV group participants to identify this data as false allows us to classify this impact as hidden. The key moments of the performed empirical study are illustrated in Figures 8–10.

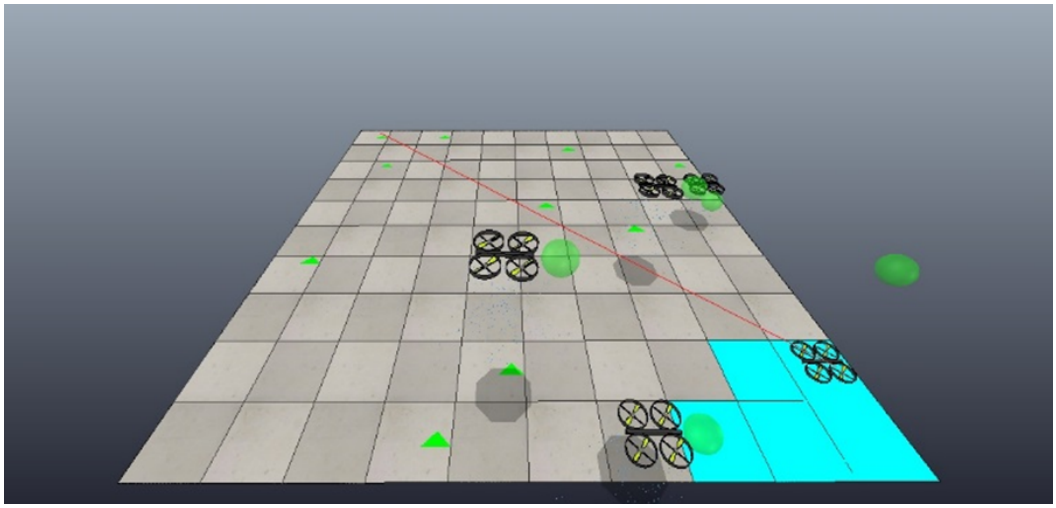

Figure 8. The empirical study initialization moment. UAVs group participants located at the zone A. Red arrow indicates task in progress.

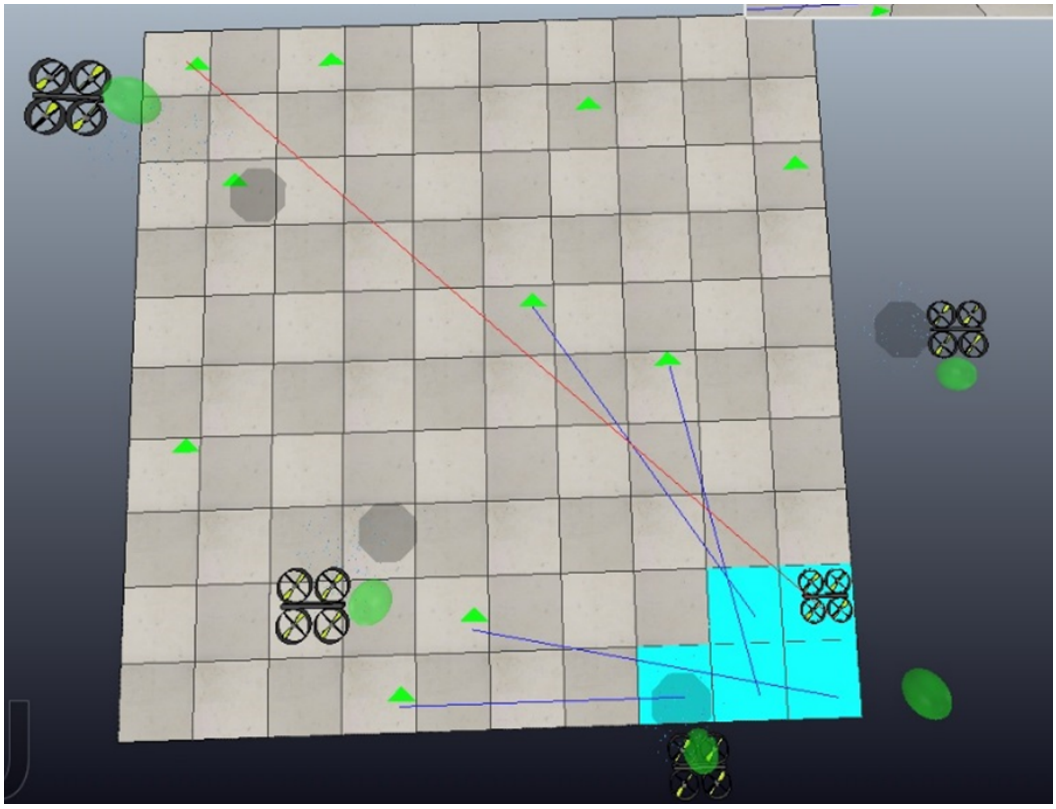

Figure 9. The process of tasks performing by the UAV group participants. Blue and red arrows indicate completed tasks and tasks in progress, respectively.

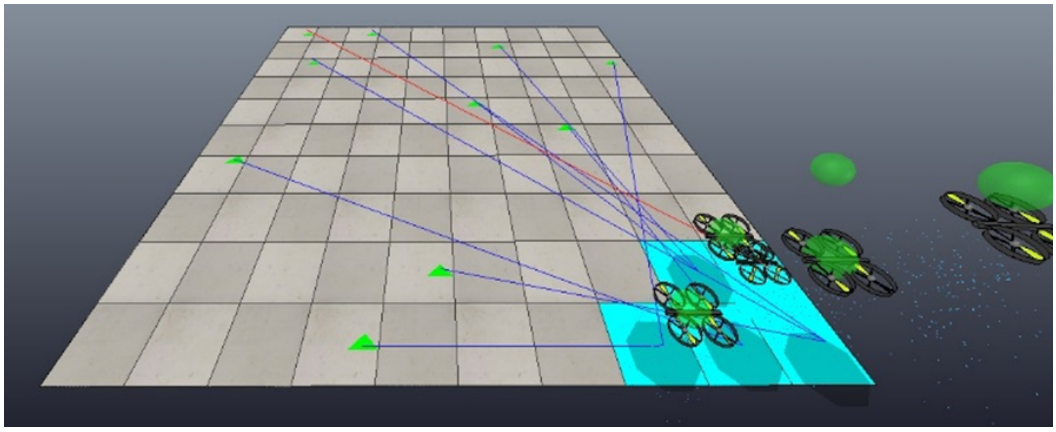

Figure 10. An example of destructive impact implementation in the UAVs intergroup communication. The "intruder" UAV was assigned the task and did not perform it; at the same time, other UAVs cannot be assigned this task, as it already was occupied by the "intruder". Blue and red arrows indicate completed tasks and tasks in progress, respectively.

6.2. Empirical Study Results

We simulated all the scenarios, described in Section 5, where the group is exposed to HDII by the UAV that provides false data. Tables 2 and 3 demonstrate the empirical study results with HDII implementation and without it. For the convenience, all the data is presented in percentages.

Table 2. Simulation results without HDII implementation.

Average Expended Energy Resources	Failed UAVs	Completed Tasks
79.2%	0%	100%

Table 3. Simulation results with HDII implementation. HDII and damage types are defined according to Section 5.

HDII Type	Average Expended Energy Resources	Failed UAVs	Completed Tasks	Damage Type
1	95.3%	0%	100%	Indirect
2	96.6%	0%	100%	Indirect
3	73.8%	0%	90%	Direct
4	96.2%	20%	90%	Indirect, Undetermined, Direct
5	59.5%	0%	90%	Direct
6	82.3%	10%	100%	Undetermined
7	96.7%	10%	100%	Indirect, Undetermined

From the results, one can see that the 1st and 2nd types of HDII showed an increase in average energy resources spent by UAVs. This can be interpreted as an indirect damage, as the implemented HDII resulted in a decrease in UAVs able to participate in the task allocation auction. The 3rd HDII type simulation showed a decrease in completed tasks, which is an outcome of the energy resources lack. In turn, the average expanded energy resources declined as a result of the remaining unperformed tasks. The 4th HDII type implementation resulted in all types of damage. By the reason of transmitting the false data on the obstacles location, UAVs selected a sub-optimal path toward the "flag", which increased the energy resources consumption and led to the crash of several UAVs. However, 90% of tasks were completed. The data on 5th HDII type simulations showed the decline in completed tasks, which was a result of the data falsification on the technical condition provided by one of the UAVs. The 6th HDII type caused undetermined damage, as a consequence of providing false data on the energy resource balance. As a result, one of the "harmless" UAVs crashed. The damage type was defined as indirect because the UAV crash led to the others group participant's energy resources consumption growth. The 7th HDII type simulations showed an increase in the UAVs average energy resources consumption. Providing the false data on other UAVs and obstacles location resulted in one of the UAVs crashing.

As one can see from Table 3, the average expended energy resources percentage can vary and depends on the particular simulation scenario. If UAVs provide false data to other participants, we assume that the group has to spend more time and resources to perform the tasks, as the tasks are allocated to inappropriate UAVs in a sub-optimal way. In HDII Type 5 experiments, UAVs provided false information on their technical state; however, comparing to other tested HDII types, HDII Type 5 resulted in a minimal average resource consumption to perform all the tasks. Here, we can conclude that when the UAV provided false data, for example, on the obstacles location or energy resources balance (other HDII types), it resulted in sub-optimal decisions in the path planning, tasks allocation, and dynamic movement adjustment.

7. Conclusions and Future Work

In our paper, we proposed our novel approach to evaluate how destructive information impact affects unmanned aerial vehicles individual and overall group performance. The concepts of internal, external and intergroup informational interaction were introduced and formalized. Informational interaction analysis allowed to define and classify hidden destructive information impact types according to the intentionality and to the impact on

the overall group performance (direct, indirect, and undetermined damage). Moreover, we provided calculus which allowed us to evaluate and quantify the damage caused by the destructive information impact. To evaluate our approach, we conducted an empirical study using the CoppeliaSim robotic simulation environment. During the simulations, we employed the hidden destructive information impact that affected the performance both of the individual unmanned aerial vehicle and the whole group.

It is worth mentioning that, in some cases, the apparent destructive information impact vulnerabilities can be neutralized or mitigated by the conventional security and safety methods, e.g., authentication and mobile cryptography. However, to address vulnerabilities related to the hidden destructive information impact, it is crucial to develop novel security and safety approaches. We believe the threats classification and attacks scenario description, provided in this work, can contribute to the development and improvement of such approaches and methods by a community.

Our further research prospects are aimed at hidden destructive information impact countermeasures developing and adjusting, modeling various attack scenario on real unmanned aerial vehicles and assessing intergroup communication reliability and tolerance in different situations. Managing these points can allow us to develop a generic intergroup communication security model for unmanned aerial vehicles, which would allow to design more attack-tolerant devices and to increase their performance in hostile environments.

Author Contributions: Conceptualization, E.M., S.C. and I.V.; methodology, E.M., S.C. and I.K.; software, I.K. and N.T.; validation, I.K. and N.T.; formal analysis, I.V.; investigation, E.M. and I.V.; resources, I.V.; data curation, I.K. and N.T.; writing—original draft preparation, S.C. and E.M.; writing—review and editing, S.C. and E.M.; visualization, E.M. and N.T.; supervision, I.V.; project administration, I.V.; funding acquisition, I.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Ministry of Science and Higher Education of the Russian Federation: No. 075-01024-21-02 from 29 September 2021 (project FSEE-2021-0014).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Guan-Zheng, T.; Huan, H.; Sloman, A. Ant colony system algorithm for real-time globally optimal path planning of mobile robots. *Acta Autom. Sin.* **2007**, *33*, 279–285.
2. Chung, T.H.; Jones, K.D.; Day, M.A.; Jones, M.; Clement, M. *50 vs. 50 by 2015: Swarm vs. Swarm uav Live-Fly Competition at the Naval Postgraduate School*; Curran Associates, Inc.: Red Hook, NY, USA, 2013; pp. 1792–1811.
3. Yakimenko, O.A.; Chung, T.H. Extending autonomy capabilities for unmanned systems with CRUSER. In Proceedings of the 28th Congress of the International Council of the Aeronautical Sciences (ICAS 2012), Brisbane, Australia, 23–28 September 2012; pp. 47–49.
4. Yang, J.H.; Kapolka, M.; Chung, T.H. Autonomy balancing in a manned-unmanned teaming (MUT) swarm attack. In *Robot Intelligence Technology and Applications 2012*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 561–569.
5. Chung, T.H.; Burdick, J.W.; Murray, R.M. A decentralized motion coordination strategy for dynamic target tracking. In Proceedings of the 2006 IEEE International Conference on Robotics and Automation, Orlando, FL, USA, 15–19 May 2006; pp. 2416–2422.
6. Tsao, K.Y.; Girdler, T.; Vassilakis, V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Netw.* **2022**, *133*, 102894. [CrossRef]
7. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
8. Lin, C.; He, D.; Kumar, N.; Choo, K.K.R.; Vinel, A.; Huang, X. Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [CrossRef]
9. Zikratov, I.A.; Vadimirovna, K.E.; Viktorovna, Z.T. Vulnerability analysis of robotic systems with swarm intelligence. *J. Sci. Tech. Inf. Technol. Mech. Opt.* **2013**, *87*, 149–154.
10. Huang, S.; Teo, R.S.H.; Tan, K.K. Collision avoidance of multi unmanned aerial vehicles: A review. *Annu. Rev. Control* **2019**, *48*, 147–164. [CrossRef]
11. Kulikov, A.; Timoshenko, A.; Zhukov, A.; Kartsan, I. Control system for multi-agent groups of heterogeneous sensors. In Proceedings of the MIP Computing-V 2022: V International Scientific Workshop on Modeling, Information Processing and Computing, Krasnoyarsk, Russia, 25 January 2022; pp. 1–6.

12. Luo, L.; Wang, X.; Ma, J.; Ong, Y.S. Grpavoid: Multigroup collision-avoidance control and optimization for UAV swarm. *IEEE Trans. Cybern.* **2021**, 1–14. [CrossRef] [PubMed]
13. Koval, E.; Lebedev, I. Obshchaya model'bezopasnosti robototekhnicheskikh sistem [General model of robotic systems information security]. *Sci. Tech. J. Inf. Technol. Mech. Opt.* **2013**, *4*, 86.
14. Viksnin, I. A model of information security for cyberphysical systems. *Sci. Bus. Ways Dev.* **2018**, *2*, 15–20.
15. Komarov, I.; Yur'eva, R.; Drannik, A.; Maslennikov, O.; Kovalenko, M.; Egorov, D. Research on destructive impact of robots-sabouters' influence on multi-agent system's productivity. *Control Process. Stab.* **2014**, *1*, 336–340.
16. Zikratov, I.; Zikratova, T.; Lebedev, I. Trust model for information security of multi-agent robotic systems with a decentralized management. *Sci. Tech. J. Inf. Technol. Mech. Opt.* **2014**, *14*, 47–52.
17. Chuprov, S.; Viksnin, I.; Kim, I.; Marinenkov, E.; Usova, M.; Lazarev, E.; Melnikov, T.; Zakoldaev, D. Reputation and Trust Approach for Security and Safety Assurance in Intersection Management System. *Energies* **2019**, *12*, 4527. [CrossRef]
18. Zikratov, I.A.; Viksnin, I.; Zikratova, T.; Shlykov, A.; Medvedkov, D. Security model of mobile multi-agent robotic systems with collective management. *Sci. Tech. J. Inf. Technol. Mech. Opt.* **2017**, *17*, 443. [CrossRef]
19. Kirichenko, V. Information security of communication channel with UAV. *Electron. Control Syst.* **2015**, *3*, 23–27. [CrossRef]
20. Rivera, E.; Baykov, R.; Gu, G. *A Study on Unmanned Vehicles and Cyber Security*; Rivera 2014 ASO: El Paso, TX, USA, 2014.
21. Hooper, M.; Tian, Y.; Zhou, R.; Cao, B.; Lauf, A.P.; Watkins, L.; Robinson, W.H.; Alexis, W. Securing commercial wifi-based uavs from common security attacks. In Proceedings of the MILCOM 2016—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; pp. 1213–1218.
22. Sidorov, V.; Ng, W.K.; Lam, K.Y.; Salleh, M. Cyber-threat analysis of a UAV traffic management system for urban airspace. In Proceedings of the Air Transport Research Society World Conference, Bordeaux, France, 5–8 July 2017; Volume 2017.
23. Watkins, L.; Ramos, J.; Snow, G.; Vallejo, J.; Robinson, W.H.; Rubin, A.D.; Ciocco, J.; Jedrzejewski, F.; Liu, J.; Li, C. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems. In Proceedings of the 1st ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, Los Angeles, CA, USA, 26 June 2018; pp. 1–6.
24. Higgins, F.; Tomlinson, A.; Martin, K.M. Threats to the swarm: Security considerations for swarm robotics. *Int. J. Adv. Secur.* **2009**, *2*, 288–297.
25. Sedjelmaci, H.; Senouci, S.M. Cyber security methods for aerial vehicle networks: Taxonomy, challenges and solution. *J. Supercomput.* **2018**, *74*, 4928–4944. [CrossRef]
26. Javaid, A.Y. Cyber Security Threat Analysis and Attack Simulation for Unmanned Aerial Vehicle Network. Ph.D. Thesis, University of Toledo, Toledo, OH, USA, 2015.
27. Kalyaev, I.; Gaiduk, A.; Kapustyan, S. *Modeli i Algoritmy Kollektivnogo Upravleniya v Gruppakh Robotov*; Fizmatlit: Moscow, Russia, 2009; 280p.
28. Chuprov, S.; Viksnin, I.; Kim, I.; Usova, M. Intersection management tasks in mobile robotic system with decentralized control. In Proceedings of the 10th Majorov International Conference on Software Engineering and Computer Systems, Saint-Petersburg, Russia, 12–13 December 2019; pp. 1–12.
29. Nanjanath, M.; Gini, M. Repeated auctions for robust task execution by a robot team. *Robot. Auton. Syst.* **2010**, *58*, 900–909. [CrossRef]
30. Gao, L.; Yu, S.; Luan, T.H.; Zhou, W. *Delay Tolerant Networks*; Springer: Berlin/Heidelberg, Germany, 2015.
31. Karnik, N.M.; Tripathi, A.R. Security in the Ajanta mobile agent system. *Softw. Pract. Exp.* **2001**, *31*, 301–329. [CrossRef]
32. Shibli, M.A.; Muftic, S. Magicnet: Security architecture for authorization of mobile agents. In Proceedings of the 3rd International Conference on Internet Technologies and Applications, ITA 09, Wrexham, UK, 8–11 September 2009; pp. 506–513.
33. Vigna, G. Protecting mobile agents through tracing. In Proceedings of the 3rd ECOOP Workshop on Mobile Object Systems, Jyväskylä, Finland, 9–13 June 1997; pp. 1–14.
34. Lee, H.; Alves-Foss, J.; Harrison, S. The use of encrypted functions for mobile agent security. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004; p. 10.
35. Page, J.; Zaslavsky, A.; Indrawan, M. A buddy model of security for mobile agent communities operating in pervasive scenarios. In Proceedings of the Second Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation, Dunedin, New Zealand, 1 January 2004; Australian Computer Society, Inc.: Dunedin, New Zealand, 2004; Volume 32, pp. 17–25.
36. Viksnin, I.I.; Schcepin, N.D.; Patrikeev, R.O.; Shlykov, A.A.; Komarov, I.I. Approaches to communication organization within cyber-physical systems. In Proceedings of the 2017 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia, 3–7 April 2017; pp. 484–490.
37. Guan, X.; Yang, Y.; You, J. POM-a mobile agent security model against malicious hosts. In Proceedings of the Fourth International Conference/Exhibition on High Performance Computing in the Asia-Pacific Region, Beijing, China, 14–17 May 2000; Volume 2, pp. 1165–1166.
38. Vigna, G. Cryptographic traces for mobile agents. In *Mobile Agents and Security*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 137–153.
39. Rohmer, E.; Singh, S.P.; Freese, M. V-REP: A versatile and scalable robot simulation framework. In Proceedings of the 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems, Tokyo, Japan, 3–7 November 2013; pp. 1321–1326.