inventions

Article

Information Protection in Complexes with Unmanned Aerial Vehicles Using Moving Target Technology

Vitaly Pikov, Anatoly Ryapukhin * and Daniela Veas Iniesta

Moscow Aviation Institute, Volokolamskoe Highway 4, 125993 Moscow, Russia
* Correspondence: ryapukhin.a.v@mail.ru

Abstract: This article is devoted to the problem of information security in complexes with unmanned aerial vehicles (UAV). Science knows a new promising method of information protection: moving target defense (MTD). The essence of this method is that due to periodic changes in the parameters of the infocommunication network the information about the information infrastructure collected by the attacker at the reconnaissance stage becomes irrelevant, and the attack becomes ineffective. This article also discusses the features and types of confidential information processed in complexes with UAV and provides a review of the experience of creating systems for protecting information from unauthorized access of complexes with UAV. The proposed hypothesis is tested using a model created using a tool: the GNS3 program. The model in the form of a test network in the GNS3 emulator recreates the proposed method. It was concluded that the effectiveness of the harmful impact on the complex with UAV was reduced by three times. The disadvantages of the proposed method include the problem of ensuring the availability of protected information resources for other legitimate, authorized participants in network interaction, as well as the need to solve the problem of choosing the optimal frequency of changing parameters.

Keywords: protection information; information security; UAV; MTD technology; aviation

Citation: Pikov, V.; Ryapukhin, A.; Veas Iniesta, D. Information Protection in Complexes with Unmanned Aerial Vehicles Using Moving Target Technology. *Inventions* **2023**, *8*, 18. https://doi.org/10.3390/inventions8010018

Academic Editors: Chien-Hung Liu and Konstantinos G. Arvanitis

Received: 15 November 2022
Revised: 12 December 2022
Accepted: 5 January 2023
Published: 11 January 2023

1. Introduction

UAV is one of the main trends in aviation in recent years. With their deceptive simplicity, these devices promise to change the world of the future. UAV is not only one or several aircraft but also a ground control station (GCS), as well as channels of information interaction. As experience shows, the level of information protection in complexes with UAV often leaves much to be desired. The classic solution often used in complexes with UAV, which consists in encrypting information transmitted over communication channels, is not optimal due to the limited computing resources of UAV.

MTD technology is a promising approach to information security, in which the information collected by an attacker during the intelligence phase becomes irrelevant. The information entropy for the attacker does not decrease and, accordingly, he does not have an advantage over the defending side [1]. The advantage is achieved by constant randomized reconfiguration of the system elements, all nodes of the network infrastructure of the UAV complex or by responding to information security events: incidents and taking actions to neutralize them. Researchers of information security in complexes with UAV note that it is necessary to constantly improve the applied approaches. Thus, by applying the technology of MTD to complexes with UAV, it is possible to increase the effectiveness of the information security process.

The object of this research is to identify the system for protecting information from unauthorized access of complexes with UAV.

The subject of the study is the methods and technologies for protecting information from unauthorized access of complexes with UAV, technology of MTD, indicators, and criteria for the effectiveness of the system for protecting information from unauthorized access of complexes with UAV.

The purpose of the work is to increase the level of security of confidential information in complexes with UAV by developing a new method that implements the technology of MTD.

In accordance with the goal, the following tasks should be solved:

- To consider the features and types of confidential information processed in complexes with UAV;
- To consider and analyze systems for protecting information from unauthorized access of complexes with UAV;
- To analyze the application of MTD technology to protect information in computer networks;
- To develop a way to improve the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using MTD technology;
- To propose an approbation option for the proposed method for improving the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using MTD technology.

The practical significance is determined by the possibility of applying in practice a new way to increase the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using MTD technology to ensure a high level of security of confidential information processed in complexes with UAV.

2. Materials and Methods

We perform an analytical review of approaches to ensure the information security of complexes with UAV. UAV is one of the main trends in the development of aviation in recent years. In their deceptive simplicity, these devices promise to change the world of the future. This is confirmed by the fact that in 2014 the Massachusetts Institute of Technology included them in the list of the ten most promising technologies of our time [2]. The number of UAV and the range of tasks they can perform are steadily growing, as is their importance.

Leading world powers are implementing long-term UAV development programs and developing industrial technologies for the production of key components, such as multi-purpose sensors, communication, and information processing systems, necessary to carry out their missions. According to the latest report from TechSci, the total revenue from the drone market is expected to skyrocket from $69 billion in 2018 to $141 billion in 2023 [3].

We consider the principles of communication and features of confidential information in the networks of complexes with UAV. Communication can be carried out between UAV and another object: the end point. This link can be called the UAV-X link, where X is the second end point. Next, we will consider various types of communication between UAV and the second point. Three main communication options used in complexes with UAV are subject to review:

- "UAV—GCS";
- "UAV—UAV";
- "UAV—Sputnik".

Communication "UAV—GCS" is the main type of communication for UAV. GCS exchanges data with UAV through uplink and downlink channels, which allows transmitting control commands and intelligence information. The scheme of this communication option is shown in Figure 1.

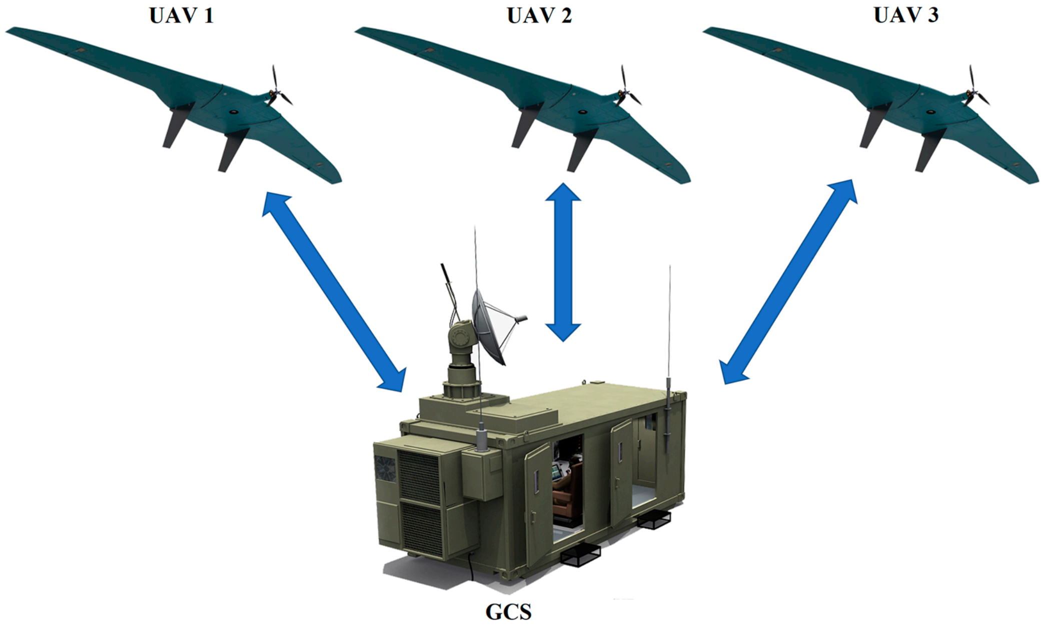

Figure 1. Scheme of the communication option "UAV—GCS".

In UAV—GCS communication, four classes of transmitted traffic are possible: control traffic, coordination traffic, sensing traffic [4], and special information.

- Control traffic includes control and monitoring commands, commands relating to a specific mission, and real-time status of UAV (for example, telemetry data, battery level, etc.);
- Coordination traffic controls the interaction between several UAV during a flight mission and tasks performed independently of GCS, for example, collision avoidance processes;
- Sensing traffic includes readings from on-board sensors that are transmitted to GCS (telemetry);
- Special information includes photos and videos.

Communication "UAV—UAV" is transferred between drones. The relay mode is also possible in cases where one UAV is out of reach of GCS, and the data is transmitted along the chain between GCS and the final UAV (Figure 2).

This communication option is the most reliable and secure compared to other categories and is often used for military purposes. In addition, satellite communications are useful over long distances without a fixed infrastructure and provide reliable and high bandwidth communications. However, it also has a number of vulnerabilities that are disclosed below.

We consider the current threats to the information security of complexes with UAV. Parallel to the development of UAV, methods and means of targeted disruption of their normal functioning are being developed. Modern technical means make it possible not only to detect and find UAV control and information collection channels but also to interfere with the operation of on-board radio-electronic equipment and ground-based automated workstations of control complexes. All this necessitated the development of cybersecurity measures in relation to complexes with UAV.

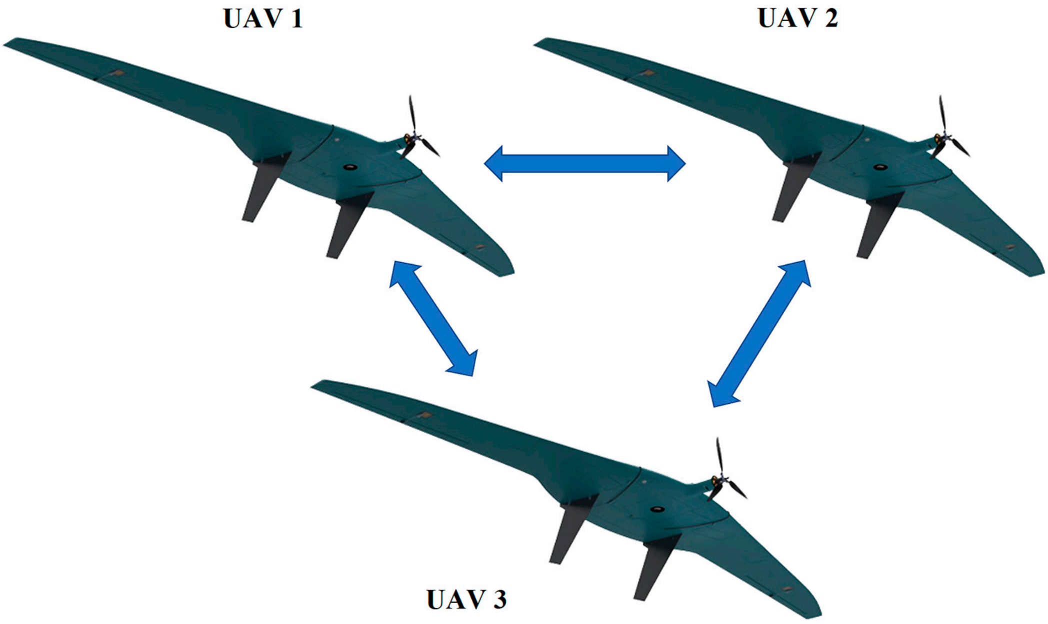

Figure 2. Scheme of the communication option "UAV—UAV".

It is worth noting that this communication option is most susceptible to jamming and Denial-of-service attack (DoS) [5–8].

In "UAV—Sputnik" communication, in long-range missions, the operator needs to determine the position of UAV for safe navigation. Therefore, UAV can establish a satellite link to collect real-time GPS position data and then transmit it back to GCS via satellite (Figure 3).

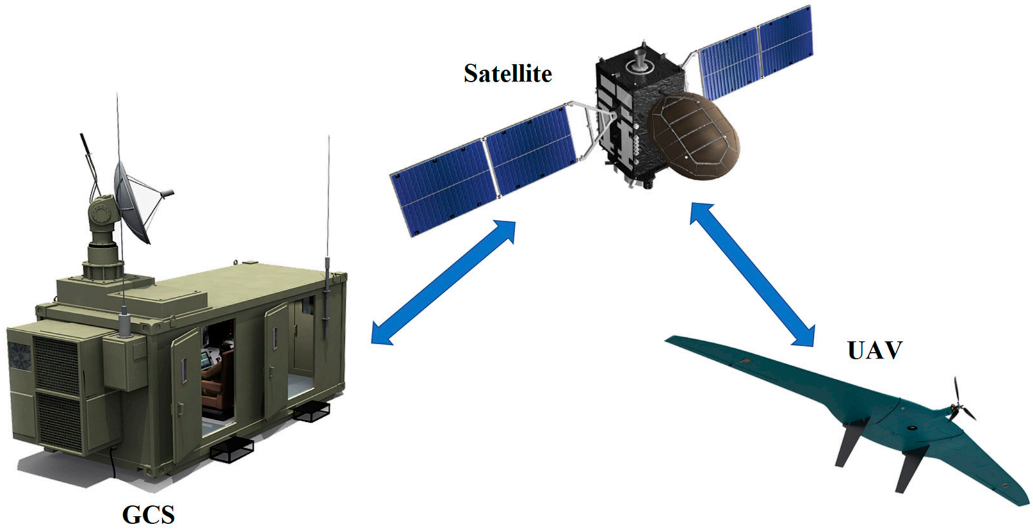

Figure 3. Scheme of communication option "UAV—Sputnik".

The information security of complexes with UAV is defined as a set of conditions under which all components of the information and control environment and the processes occurring in it are protected from the maximum possible number of threats and impacts with undesirable consequences. With the very rapid improvement of technical means and the saturation of various areas of human activity with modern information systems, the role of cybersecurity is increasing significantly [9,10]. Unmanned communications face specific security challenges along with general cyber threats. One of the reasons for the specificity of problems is that it is difficult to dynamically and adaptively solve or prevent unforeseen problems.

Some of the security threats discussed below are more specific to drones, while relatively general issues are discussed based on how adversaries can use them to threaten the use of drones.

DoS is the most common and simple type of attack that an adversary can use to prevent a drone from functioning normally. In addition, this is the fastest way to make an UAV network useless and sometimes even harmful [11]. Figure 4 shows the basic scheme of how DoS works in the case of communication with drones. Due to the large number of unnecessary requests, access to shared resources is limited for legitimate users. This leads to an overload of the system and to the refusal of some or all legitimate requests. In this process, the network connection between the ground controller and UAV is deauthenticated since the adversary sends so many data packets that this leads to a failure of computing power [12]. Data packets can be easily generated by any packet generating application (“Hping3” [13]) and sent directly to the drone’s network. It is also possible that one of the sent data packets contains malicious code that can be used to attack the drone.

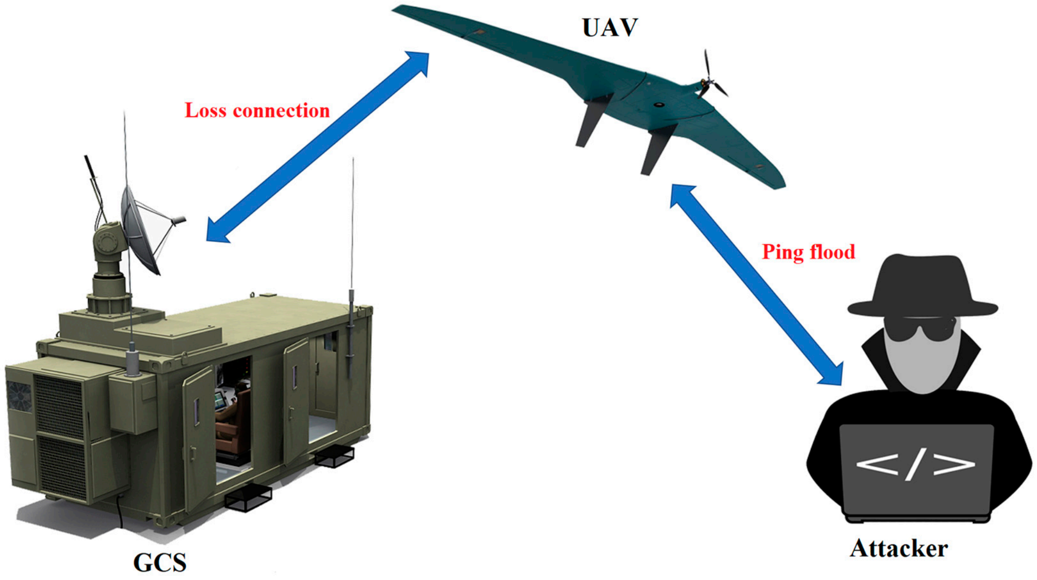

Figure 4. UAV DoS scheme.

Spoofing can be performed using multiple transmit antennas, whereby the attacker’s transmit antenna is combined with the corresponding receiver antenna and transmits false signals. In this process of obtaining GPS coordinates of the drone, it is determined by the satellite using GPS, and then its coordinates are sent to the ground controller. Counterfeiting military drones is relatively difficult because they are equipped with encryption mechanisms. Spoofing can be performed using multiple transmitting antennas [13], where the attacker’s transmitting antenna is combined with the corresponding receiving antenna and transmits false signals. An attacker can take the drone to any trajectory they want without even giving the controller a hint, since the fake coordinates are sent to the controller at regular intervals. This technique can be used to slow down the drone’s speed, making it less useful.

In a GPS spoofing attack, UAV—Sputnik communication requires incoming signals from GPS satellites, two-way communication between the drone and the ground station, as well as signals notifying the presence of the drone (Figure 5) [14].

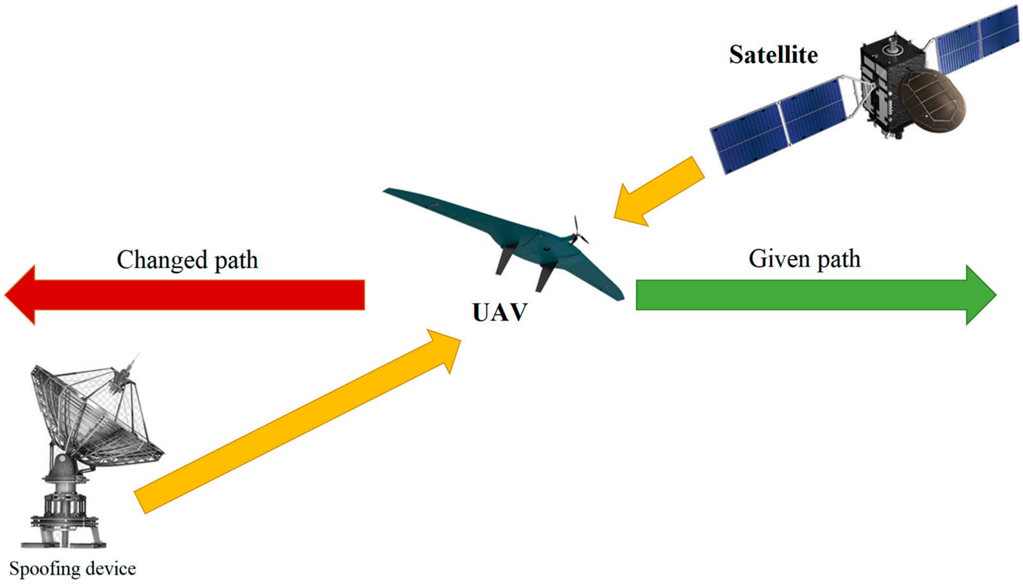

Figure 5. Scheme of GPS spoofing attacks on UAV.

The authors of [15] used software-defined radio platforms to simulate GPS in order to transmit false signals to the target drone. This methodology has long been used to hack or transmit incorrect information via drones. Using this approach, they redirect and take control of drones whose flight path depends on GPS.

According to [16], on 5 December 2011, an American UAV was detected and shot down by Iranian forces near the city of Kashmar in northeastern Iran. According to American officials, the UAV was tricked into flying over Iran. The attackers hacked UAV and entered incorrect GPS coordinates into it. This incident led to the disruption of relations between two countries. The military drone reportedly used an inertial navigation system rather than GPS navigation due to increased spoofing and jamming. Despite measures taken to prevent any spoofing attacks or to protect sensitive information available from drones, the Iranians claimed they could access it and reverse-engineered the entire drone to create their own Saegheh drones.

In "man in the middle" attack, the most well-known attack [17], the adversary controls the UAV—GCS wireless channel and changes benign packets to malicious ones, which is sometimes called "poisoning" of the communication channel (Figure 6) [18].

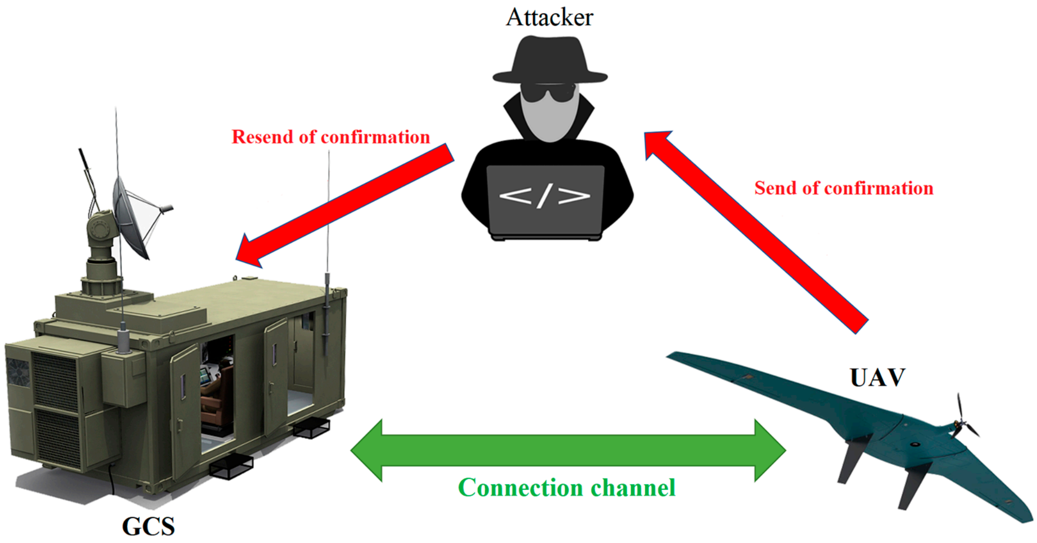

Figure 6. Scheme of the "man in the middle" attack on UAV.

Thus, the enemy can act as a link between the drone and GCS and disrupt their bidirectional communication. An example of such an attack is the "replay attack", when an adversary deceives the operator by transmitting malicious live broadcast data, for example, using the VideoJak tool [19].

3. Results and Discussion

We evaluate modern approaches to ensuring the information security of UAV. Drones use radio signals to communicate with the controller. The controller sends radio signals through the transmitter, and the drone receives them through the receiver. The radio signals between them can be jammed or spoofed.

According to an IBM researcher, drones can be easily hijacked if they do not have encryption on their on-board chips [14]. Due to the limited resources of drones, encryption will not be the ideal solution. With a huge amount of data exchange in the process of drone communication, encryption and decryption using complex algorithms require certain computing power. Security issues become even more serious if drones use Wi-Fi for communication.

A new direction in the field of drone security is the Internet of Drones (IoD). This concept is equally popular in military and commercial drones [20]. There are fundamental security and privacy concerns in drone technology related to their design. The main issues identified in the field of IoD security are privacy leakage, data privacy, data protection, data flexibility, data availability, and data encryption and decryption strategies.

The problem of the hijacking of drones and UAV is a common threat for commercial drones, which is specifically studied in [21,22]. Measures to counteract the problem of hacking and hijacking drones and other UAV are proposed in [23]. GPS spoofing is a common problem with a reliable solution. Several other studies on drone hijacking are also discussed in [24,25]. The analysis of the above sources showed that the existing solutions are not optimal, and researchers have yet to develop the best solutions for protecting UAV.

Review articles [26–28] provide a comprehensive overview of UAV security and privacy issues. UAV safety issues are thoroughly analyzed at various levels: sensor level, hardware level, and software level. In addition, UAV privacy issues, threats, and possible solutions were discussed. Possible directions for future research are presented. In the above works, the researchers come to the conclusion that it is necessary to continue to explore and develop new approaches to ensuring the security of information in the systems of complexes with UAV. An example of such a promising approach is the MTD technology, which proactively creates an advantage for the defending side in relation to the attackers [29] but has not yet been considered in the context of UAV and complexes with UAV.

An important note to all of the above is that due to the new realities in the Russian Federation and the even greater role of import substitution, most of the existing foreign solutions may not be available for use. Based on this, we can conclude that in order to ensure the process of protecting information in networks of complexes with UAV, it is necessary to develop new promising methods for protecting information in complexes with UAV using new promising approaches, which is the technology of MTD.

One of the main problems in the field of information security is that the "protection" side comes second. Often, it has to respond to the actions of an attacker with a limited amount of time and information, whereas time plays into the hands of a cybercriminal: he can conduct network reconnaissance and then carefully plan his attack.

At the same time, an attacker can identify existing vulnerabilities and take advantage of them or develop tools to bypass the security system. In addition, the implementation of protection tools in practice is often far from ideal, which gives attackers even more opportunities to exploit the system. A 2016 report predicts that by 2020, 99% of exploited vulnerabilities will be known to security and IT professionals a year ago [30]. The main reason for this is the time and complexity associated with routine maintenance and fixing vulnerabilities in the underlying infrastructure.

In order to balance the capabilities of the defending side, MTD technology was developed that solves this fundamental problem in two approaches:

- A constant dynamic reconfiguration of the protected system;
- Taking countermeasures that make the attack impossible once it has been determined.

Both approaches described above lead to the fact that the information collected during the exploration phase becomes irrelevant [31]. The information entropy for the attacker does not decrease and, accordingly, it does not have an advantage over the defending side. At the same time, it should be taken into account that the reconfiguration mechanism cannot be deterministic, since the attacker, having time on his side, will conduct a sufficient analysis of the security system and develop his attacks accordingly, which will make the use of MTD technology ineffective. Therefore, MTD methods should always have implicit randomness built into them.

We define the strategies of MTD technology in complexes with UAV. MTD strategies in combination with UAV can be roughly divided into three categories:

- MTD at the network level, which changes the way it functions, for example, using IP hopping technique, in which IP address changes periodically, or we use random port numbers and fake hosts;
- MTD at the host level is directed to changes in the host, for example, to a periodic change in configuration or name;
- MTD at the application level changes their types and versions and randomizes the location of address space layout randomization (ASLR) and the source code with compilation processes.

Thus, MTD system, $\sum$, is the ordered set of (σ, G, P), where σ is the configurable system, G is the set of operational security goals and objectives, and P represents the security policies. Therefore, σ is the set of (S, A, τ), where S = (s_1, s_2, . . . , s_n) is the set of system states in which it can be, A = (α_1, α_2, . . . , α_n) is the set of actions to take, and τ:S × A→S is the system state transition function. The system state s is a unique assignment of the value z from the configuration parameter type Π to the configuration parameter π. The type of the configuration parameter Π denotes the range of possible values that the configuration parameter π can take. The configuration parameter π can take on a value based on its configuration type Π to define configuration details. An example of host Π configuration is shown in the diagram (Figure 7).

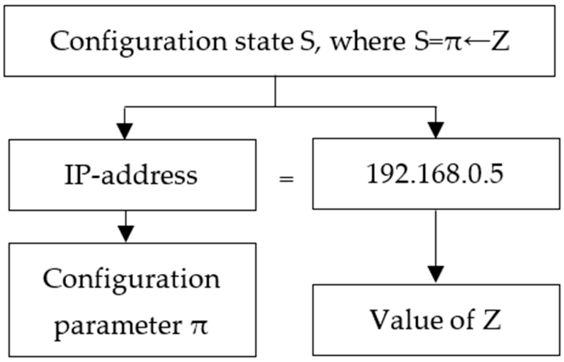

Figure 7. Host Π configuration example.

We define the surfaces of the network infrastructure for the implementation of MTD technology in combination with UAV. Network and cloud infrastructure in the context of MTD technology are considered as four surfaces:

- Exploration surface;
- Attack surface;
- Detection surface;
- Prevention surface.

The surface refers to the high-level part of the system that is available for attack. The alleged adversary first tries to probe the target network, trying to figure out its topology, bandwidth, software, deployment on various nodes, etc. All this knowledge helps the enemy to carry out an attack and helps him move to different points of the network and collect and manage important information. Next, we will analyze the motivation behind the need to make each of these surface dynamic.

In exploration surface, the main reason for shifting the intelligence surface is to make sure that the information an attacker can gather by scanning open ports, sending non-malicious traffic to reveal system topology, discover vulnerabilities, etc., is noisy or inaccurate. Thus, the enemy, having this inaccurate information from intelligence, will be forced to shoot arrows (attacks) at our MTD blindly. In [32], Al-Shaer et al. argue that network attacks using intelligence can allow an attacker to obtain an IP address and port numbers. To deprive them of this advantage, the authors propose the concept of random host mutation (RHM). In RHM, MTD nodes are assigned random virtual IP (vIP) addresses in an unpredictable and distributed manner.

In attack surface, the main purpose of switching between attack surfaces is to invalidate the attack that the attacker has prepared. A textbook example of such a surface shift is a situation in which an attack that exploits vulnerability in a Linux-based operating system (OS) becomes useless; by the time it is implemented, defenders have transferred the protected system to Windows OS. For example, in [33], researchers are developing a MTD system that switches between different OS. The authors in [34] consider a similar concept by implementing MTD, which can perform OS rotation at a given frequency for machines using a centralized mechanism.

In [35], system states consist of variables, each of which indicates whether a certain vulnerability in the network infrastructure has been exploited (or not) and based on this decides when and how to act. Similarly, the authors in [36] move a deployed virtual machine to another physical server if the impact of known vulnerabilities (measured using certain metrics) on the physical server exceeds a threshold. In [37], the authors implement an MTD where they move services deployed on a particular virtual machine (VM) to another VM. A logical development of their ideas could be to use both approaches to develop a hybrid MTD that moves both services between VMs and VMs between real physical servers in a cloud network, resulting in a multi-layer MTD.

In detection surface, the need to detect attacks based on the nature of traffic on the network and the behavior or types of requests on the host machine is the basis of cybersecurity. The main problem arising from this is finding a balance between the effectiveness of protection and minimizing the impact on system performance.

One part of the works studying the mobilization of the detection surface is focused on maintaining the effectiveness of these intrusion detection systems while reducing their impact on performance. In [38,39], the authors show that when faced with stealthy botnets or external adversaries that are strong enough to attack any internal node of a deployed system, shifting the detection surface helps maintain system performance while effectively detecting an ongoing attack.

Another logical direction for studying the mobility of the detection surface is to increase its efficiency. In [40], the authors use a set of classifiers that can distinguish a letter from spam and switch between them to make it more difficult for an attacker to deceive the system.

In prevention surface, the purpose of MTD, which shifts the surface of prevention, is to make the attacker's process costly by introducing uncertainty about the system's effective defense mechanism. For example, it becomes difficult for an adversary to understand if his attack is undetected and therefore passed through the real system or if it was detected and is currently being tracked in a honeynet environment.

Research on MTD methods for shifting the avoidance surface has been sparse, especially in the context of computer networks. The problem with this direction is mainly due to the fact that the administrator can use these protections only when he is able to identify an attack with high accuracy and identifying attacks in it is a strong assumption. In [41], the authors make this assumption and propose a MTD mechanism that changes network bandwidth in response to malicious activity.

We formulate the very method of increasing the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using the technology of MTD. Thus, based on the foregoing, including the previously given conceptual apparatus on the subject of MTD technology, we need to increase the information entropy for the attacker by giving mobility to one or more surfaces of the drone network infrastructure. Thus, not only UAV will move in space, making it difficult to conduct a cyberattack on it, but also the components within UAV network will change in a way randomized for the attacker but predetermined for the legitimate participant in the process.

As a part of this work, it was decided to focus on the exploration surface and an approach similar to the previously mentioned IP hopping because it is considered the most studied and effective method of all that MTD technology has to offer at the moment. When using these approaches, the system's exposure to external threats is significantly reduced, which makes it difficult for the enemy to find vulnerable targets in a protected infrastructure. Additionally, even if such targets are discovered, the knowledge gained can only be used for a very short period of time, since the secure MTD network will continue to change its parameters. Thus, we reduce the likelihood of a successful attack even at the reconnaissance stage.

In addition, it is worth considering that the most common DoS is performed by sending ICMP packets to IP addresses. Accordingly, the enemy will need not only to have time to determine the current address but also to launch an attack on it. An attacker most likely will not expect a change in the system parameters, and at the same time, he has a limited period of time to prepare and conduct an attack due to the active movement of UAV.

Based on this, in order to increase the effectiveness of the process of ensuring information security in the networks of complexes with UAV, it is necessary to:

- Develop new or certify ready-made solutions using MTD technology;
- Adapt these solutions, taking into account the peculiarities of networks of complexes with UAV;
- Test previously adapted solutions in order to evaluate their effectiveness.

We propose a variant of approbation of the proposed method for improving the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using MTD technology.

The approach proposed earlier will be tested using the graphic network simulator 3 (GNS3) tool [42]. The choice in favor of this network emulator was made, guided by the following statements:

- The tool should demonstrate realistic network behavior;
- It is necessary to be able to use real network security or introduction testing tools on the network;
- It is necessary to be able to flexibly configure all the necessary parameters and elements of the network.

Network simulators OMNET++ [43] or NS-3 [44] cannot be taken into account due to inconsistency with the second point. While GNS3, which is widely used to create, design, and test a network in a virtual environment, offers an easy way to design and create networks of any size without the need for hardware and meet all the requirements put forward. GNS3 is highly flexible and can handle most network tasks. It supports various types of virtualized devices and can be easily administered using a graphical interface. A graphical user interface may be installed remotely from the actual environment, which may run on a different computing platform and thus may use, for example, cloud computing resources.

The above properties allow creating a model of the topology of the network of complexes with UAV without resorting to hardware implementation in order to test the proposed approach.

We create a network model of the UAV complex. In the previously described graphical network simulator, the network model of an UAV complex was recreated, as shown in Figure 8, and consisted of four subnets:

- Attacker’s network, which includes an attacker, a switch, and a router. In this topology, it is an attacker connected to UAV-1. At the same time, it is important to note that the question of the mechanism for the appearance of a malicious participant in network interaction remains outside the scope of this work;
- Network of the first UAV, which includes three hosts representing two sensors and a flight controller host; in addition, there is a switch and a router. It is connected to the ground control network;
- Network of the second UAV, similar to the network of the first UAV, which also includes two hosts that are sensors, a flight controller host, a switch, and a router. It is connected to a GCS network;
- GCS network includes a host of GCS, a switch, and a router connected for both drones.

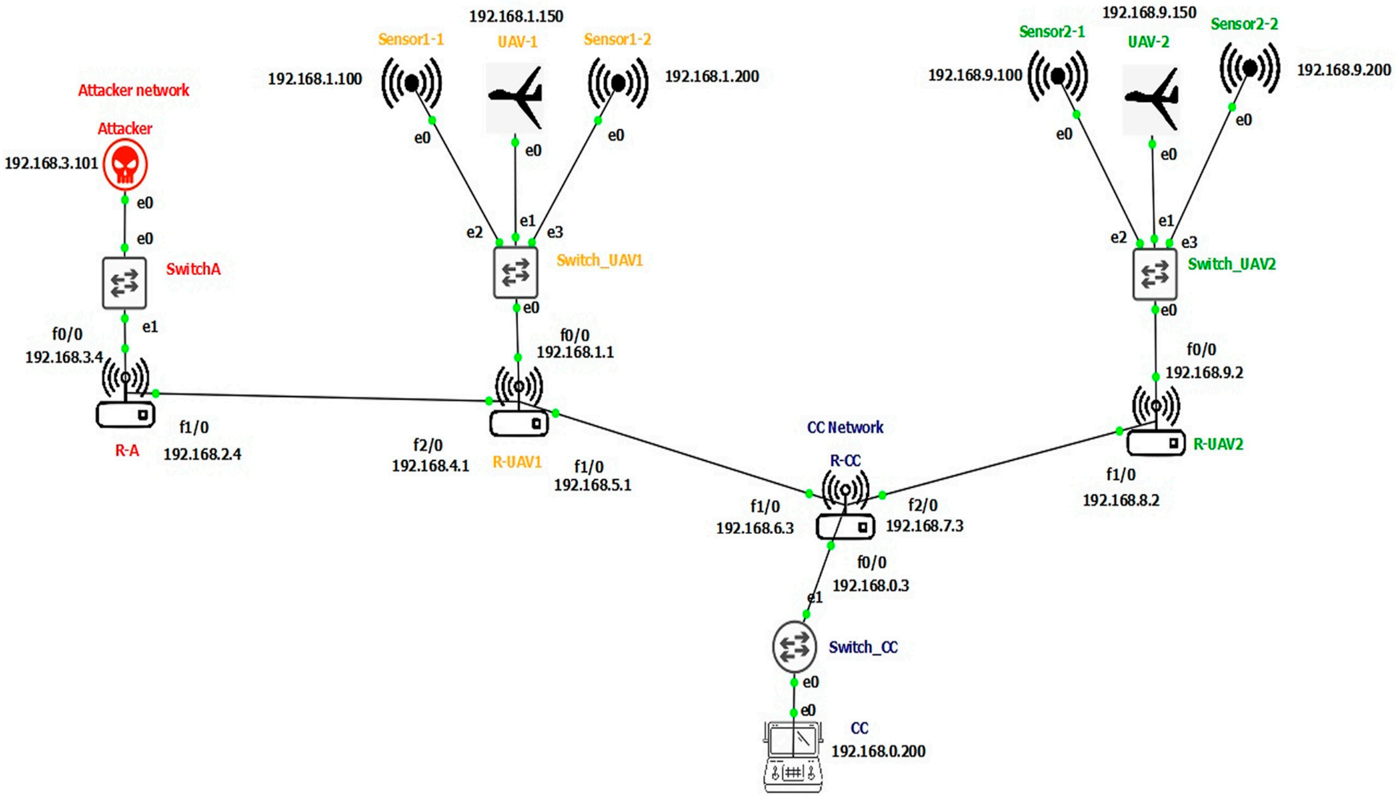

Figure 8. Topology of the test network at the stand.

Since this network emulation environment does not support wireless communication protocols, it was decided to replace them with ethernet connections. This will not affect the results of testing due to the fact that vulnerabilities and problems of wireless communication formats are not considered in the context of this work, and the very fact of connection and availability of hosts by IP address is important for project implementation. Simple ethernet switches were used as switches, and Cisco 7200 series routers were used. A virtual PC simulator [45] was used for sensor hosts and GCS; they were only required to be able to transmit data to flight controller hosts and check the availability, so these “light” PCs with support for DHCP protocol and ping were used. For the key elements of the system, controller hosts, ParrotOs distribution [46] was used, which is Linux distribution based on Debian with a focus on computer security. It is designed for penetration testing, vulnerability assessment, mitigation, and anonymous web browsing. This choice was made due to the many built-in penetration, system, and network monitoring tools. Thus, a model of the network topology was formed, including UAV—GCS connection.

In order to demonstrate the application of the ideas of MTD technology in the context of networks of complexes with UAV, it was decided to develop a project implementation of the proposal, which consists in a constant randomized change in IP addresses of the flight controller host. At the same time, in order for legitimate network participants to continue interacting with this device, it is assumed that before changing the address, the next address being prepared for use will be sent via an encrypted communication channel.

Returning to the previously introduced framework, in our configurable system σ, system state set S is 252 (255 possible IP address states minus those already in use by other legitimate hosts), and action set A consists of a single action. The system state s changes with a given period of 40 s, and the configuration parameter π is an IP address that takes the random value z. In order to increase the information entropy, the period of change in the state of the system s can be reduced, but then the informational interaction of legitimate network participants will be difficult. With the further development of the project, it will be necessary to analyze and select the most effective period of time for changing the network parameter.

Thus, a method was implemented to improve the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using MTD technology.

First, we will evaluate the effectiveness of the protection of the complex with UAV without the use of MTD technology. In the first stage of the experiment, on the part of the attacking host, we will scan the network using the nmap tool [47] to determine the targets of the attack and, directly, we will perform the ping flood attack using the previously mentioned hping3 tool.

This tool is capable of sending custom ICMP/UDP/TCP packets and displaying the target's replies, just like ping does with ICMP replies. It supports fragmentation, arbitrary content, and packet size, and can be used to transfer files over supported protocols.

Inside the emulator model, using the limited resources of the system, a load was created, on average, equal to 1950 Kb/s, which is already a problem for the limited resources of UAV network. In a real scenario, this load will increase many times because there will be no previously mentioned limiting elements. In addition, DoS can become distributed as a denial-of-service attack (DDoS), which greatly increases the potential load.

Secondly, we will evaluate the effectiveness of the protection of the complex with UAV using MTD technology. Approbation of the proposed measures was built as follows:

- Design implementation was installed on the host flight controller of subnet of UAV №1. Sensor hosts send simple ping requests to the host controller, and the host controller sends requests to GCS to emulate normal traffic and check the availability of devices;
- An UAV №2 subnetwork host flight controller has standard security settings, no design implementation has been installed on it, and these hosts communicate with each other in the same way as UAV №1 network;
- At a random time, the attacker scans the network of UAV №1, determines the hosts, and launches an attack on the host flight controller; this process is repeated 10 times to obtain average results.

Actions similar to item 3 are repeated for UAV №2.

As a result, out of 10 attacks on UAV №1, only 3 turned out to be successful because, on average, the attacker scans the subnet and starts the attack at the detected address on average every 35 s. Thus, in seven cases, the host had time to switch to a new configuration, and the attack was carried out using outdated data. Attacks on UAV №2 were successful in 10 out of 10 cases, and the load on the network was similar to the previous item.

For the final testing, a model was built using Excel, the results of which are shown in Figure 9.

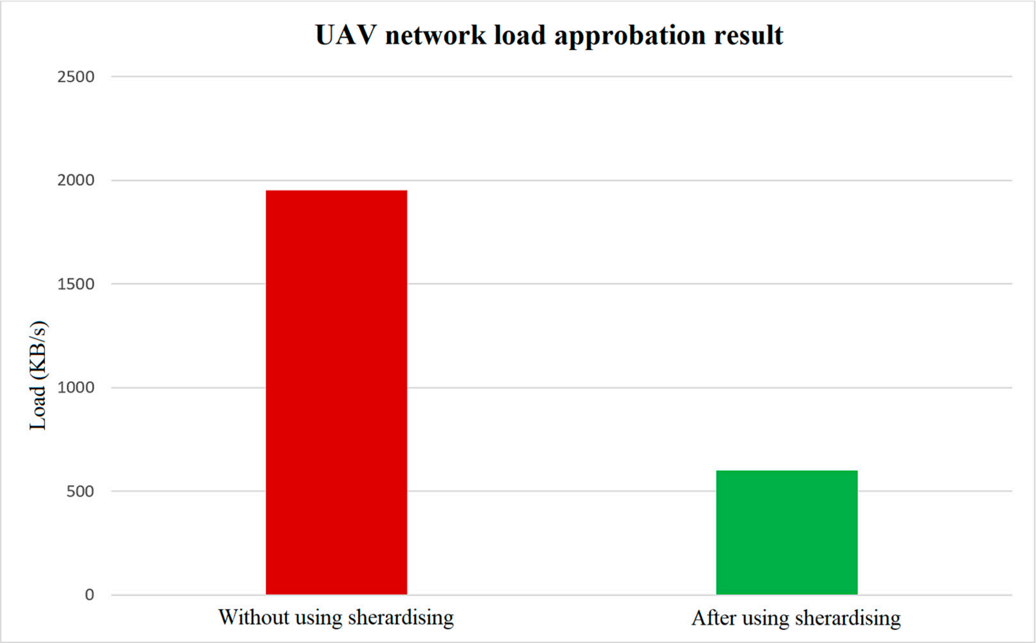

Figure 9. Result of approbation of the proposed measures.

Based on the above graph, we can see that, on average, for 10 analyzed events, the load on the network is 3 times less when using MTD technology.

The disadvantages of the proposed method include the emerging problem of ensuring the availability of the protected element of the system for other legitimate network participants. In addition, in the current implementation, it is not known which parameter change period is optimal. In the future, the design implementation will have to solve this problem, as well as ensure continuous communication between all network elements of the complex with UAV [48].

4. Conclusions

The trend and exponential growth in the use of UAV are giving rise to the era of autonomous aircraft. UAV offer numerous advantages for civilian and military applications. By contrast, the problems of ensuring the information security of complexes with UAV are gradually increasing due to limited resources. It is worth remembering that it will always be easier to use means of attack than to build protection against them.

In this paper, we propose a new way to increase the level of information security of complexes with UAV, which implements the technology of MTD.

In addition, the following tasks were solved:

- The features and types of confidential information processed in telecommunication systems and networks of complexes with UAV are considered;
- The information security systems of telecommunication systems and networks of complexes with UAV are considered and analyzed;
- The application of MTD technology for information protection in computer networks is considered;
- The method to improve the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using MTD technology has been developed;
- The variant of approbation for the proposed method for improving the effectiveness of the system for protecting information from unauthorized access of complexes with UAV using the technology of MTD is proposed.

Summing up, we can say that the creation of new attack and protection technologies in the field of information security will continue indefinitely due to the fact that there is a need to ensure the security of confidential (protected) information. With the application of MTD technology, the initiative is finally in the hands of the defending side, and the potential of these techniques can be unlimited.

The method of information protection proposed in the study of complexes with UAV using the technology of a moving target, when implemented in practice, does not impose any restrictions on the size of UAV, as well as its scope (military or civil purposes).

With the further development of complexes with UAV, it is necessary to take care of ensuring their safety. With the increase in resources and performance of such devices, researchers will have more scope to apply new and previously known techniques, which will allow not only to keep up with the development of attacks but also to increasingly seize the initiative to make truly secure and trusted devices capable of performing tasks in conditions in which a person would not be able to cope.

Author Contributions: Conceptualization, D.V.I.; methodology, V.P. and A.R.; software, V.P. and D.V.I.; validation, V.P., A.R. and D.V.I.; formal analysis, A.R.; investigation, V.P.; resources, A.R.; data curation, D.V.I.; writing—original draft preparation, V.P. and D.V.I.; writing—review and editing, V.P., A.R. and D.V.I.; visualization A.R.; supervision A.R.; project administration, A.R.; funding acquisition, V.P., A.R. and D.V.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Ryapukhin, A.V.; Karpukhin, E.O.; Zhuikov, I.O. Method of Forming Various Configurations of Telecommunication System Using Moving Target Defense. *Inventions* **2022**, *7*, 83. [CrossRef]
2. Breakthrough Technologies 2014. MIT Technology Review. Available online: https://www.technologyreview.com/10-breakthrough-technologies/2014/ (accessed on 15 November 2022).
3. Global Drones Market Report. TechSciResearch. Available online: https://www.techsciresearch.com/report/global-drones-market/1345.html (accessed on 15 November 2022).
4. Andre, T.; Hummel, K.A.; Schoellig, A.P.; Yanmaz, E.; Asadpour, M.; Bettstetter, C.; Grippa, P.; Hellwagner, H.; Sand, S.; Zhang, S. Application-driven design of aerial communication networks. *IEEE Comm. Mag.* **2014**, *52*, 129–137. [CrossRef]
5. Dinger, J.; Hartenstein, H. Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration. In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 20–22 April 2006; pp. 1–8. [CrossRef]
6. Mushtaq, M.F.; Jamel, S.; Deris, M.M. Triangular Coordinate Extraction (TCE) for Hybrid Cubes. *J. Eng. Appl. Sci.* **2017**, *12*, 2164–2169.
7. Rowaihy, H.; Enck, W.; McDaniel, P.; La Porta, T. Limiting sybil attacks in structured p2p networks. In Proceedings of the IEEE INFOCOM 2007—26th IEEE International Conference on Computer Communications, Anchorage, AK, USA, 6–12 May 2007; pp. 2596–2600.
8. Naoumov, N.; Ross, K. Exploiting p2p systems for ddos attacks. In Proceedings of the 1st International Conference on Scalable Information Systems, Hong Kong, China, 30 May–1 June 2006; p. 47-es.
9. Podkorytov, A.; Ryapukhin, A. The reduction of computational cost in GNSS data network processing. *AIP Conf. Proc.* **2022**, *2467*, 030028.
10. Burova, A.; Ryapukhin, A. Reduction of the number of multiplication operations in digital signal processing algorithms by classical methods of discrete Fourier transform. *AIP Conf. Proc.* **2021**, *2402*, 040002.
11. Alladi, T.; Chamola, V.; Zeadally, S. Industrial control systems: Cyberattack trends and countermeasures. *Comp. Comm.* **2020**, *155*, 1–8. [CrossRef]
12. Chen, J.; Feng, Z.; Wen, J.Y.; Liu, B.; Sha, L. A container-based DoS attack-resilient control framework for real-time UAV systems. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 25–29 March 2019; pp. 1222–1227.
13. Hping3. Available online: https://www.kali.org/tools/hping3 (accessed on 15 November 2022).
14. Vattapparamban, E.; Güvenç, I.; Yurekli, A.I.; Akkaya, K.; Uluağaç, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 216–221.
15. Gaspar, J.; Ferreira, R.; Sebastião, P.; Souto, N. Capture of UAVs through GPS spoofing. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; pp. 21–26.

16. Iran Hijacked US Drone, Says Iranian Engineer. Available online: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer (accessed on 15 November 2022).
17. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man in the Middle Attacks. *IEEE Comm. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
18. Rodday, N.M.; Schmidt, R.D.O.; Pras, A. Exploring security vulnerabilities of unmanned aerial vehicles. In Proceedings of the NOMS 2016—2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 25–29 April 2016; pp. 993–994.
19. VideoJak: Hijacking IP Video Calls. Available online: http://videojak.sourceforge.net (accessed on 15 November 2022).
20. Ozmen, M.O.; Yavuz, A.A. Dronecrypt-an efficient cryptographic framework for small aerial drones. In Proceedings of the MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 1–6.
21. Rango, A.; Laliberte, A.; Steele, C.; Herrick, J.E.; Bestelmeyer, B.; Schmugge, T.; Roanhorse, A.; Jenkins, V. Using unmanned aerial vehicles for rangelands: Current applications and future potentials. *Environ. Pract.* **2006**, *8*, 159–168. [CrossRef]
22. Jumaat, N.F.H.; Ahmad, B.; Dutsenwai, H.S. Land cover change mapping using high resolution satellites and unmanned aerial vehicle. *IOP Conf. Ser.: Earth Environ. Sci.* **2018**, *169*, 012076. [CrossRef]
23. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
24. Johnson, L.K.; Dorn, A.W.; Webb, S.; Kreps, S.; Krieger, W.; Schwarz, E.; Shpiro, S.; Walsh, P.F.; Wirtz, J.J. An INS Special Forum: Intelligence and drones/Eyes in the sky for peacekeeping: The emergence of UAVs in UN operations/The democratic deficit on drones/The German Approach to Drone Warfare/Pursuing peace: The strategic limits of drone warfare/Seeing but unseen: Intelligence drones in Israel/Drone paramilitary operations against suspected global terrorists: US and Australian perspectives/The 'Terminator Conundrum'and the future of drone warfare. *Intell. Natl. Secur.* **2017**, *32*, 411–440.
25. Cavoukian, A. *Privacy and Drones: Unmanned Aerial Vehicles*; Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2012.
26. Mekdad, Y.; Aris, A.; Babun, L.; Fergougui, A.E.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A Survey on Security and Privacy Issues of UAVs, 2021. Available online: https://arxiv.org/abs/2109.14442 (accessed on 15 November 2022).
27. Majeed, R.; Abdullah, N.A.; Mushtaq, M.F.; Kazmi, R. Drone security: Issues and challenges. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. Available online: https://www.researchgate.net/publication/352086927_Drone_Security_Issues_and_Challenges (accessed on 15 November 2022). [CrossRef]
28. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
29. Lei, C.; Ma, D.H.; Zhang, H.Q. Optimal strategy selection for moving target defense based on Markov game. *IEEE Access* **2017**, *5*, 156–169. [CrossRef]
30. Gartner's Top 10 Security Predictions 2016. Available online: https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/ (accessed on 15 November 2022).
31. Lei, C.; Zhang, H.Q.; Tan, J.L.; Zhang, Y.C.; Liu, X.H. Moving Target Defense Techniques: A Survey. *Secur. Commun. Netw.* **2018**, *2018*, 3759626. [CrossRef]
32. Al-Shaer, E.; Duan, Q.; Jafarian, J.H. Random host mutation for moving target defense. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Berlin, Germany, 3 September 2012; pp. 310–327.
33. Carter, K.M.; Riordan, J.F.; Okhravi, H. A game theoretic approach to strategy determination for dynamic platform defenses. In Proceedings of the First ACM Workshop on Moving Target Defense, Scottsdale, AZ, USA, 3 November 2014; pp. 21–30.
34. Thompson, M.; Evans, N.; Kisekka, V. Multiple OS rotational environment an implemented moving target defense. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 September 2014; pp. 1–6.
35. Chowdhary, A.; Pisharody, S.; Huang, D. SDN based scalable MTD solution in cloud network. In Proceedings of the 2016 ACM Workshop on Moving Target Defense, Vienna, Austria, 24 October 2016; pp. 27–36.
36. El Mir, I.; Chowdhary, A.; Huang, D.; Pisharody, S.; Kim, D.S.; Haqiq, A. Software defined stochastic model for moving target defense. In Proceedings of the International Afro-European Conference for Industrial Advancement, 18 August 2017; pp. 188–197.
37. Debroy, S.; Calyam, P.; Nguyen, M.; Stage, A.; Georgiev, V. Frequency-minimal moving target defense using software-defined networking. In Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, USA, 15–18 February 2016; pp. 1–6.
38. Venkatesan, S.; Albanese, M.; Cybenko, G.; Jajodia, S. A moving target defense approach to disrupting stealthy botnets. In Proceedings of the 2016 ACM Workshop on Moving Target Defense, Vienna, Austria, 24 October 2016; pp. 37–46.
39. Sengupta, S.; Chowdhary, A.; Huang, D.; Kambhampati, S. Moving target defense for the placement of intrusion detection systems in the cloud. In Proceedings of the International Conference on Decision and Game Theory for Security, Seattle, WA, USA, 29–31 October 2018; pp. 326–345.
40. Colbaugh, R.; Glass, K. Predictability-oriented defense against adaptive adversaries. In Proceedings of the 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, Korea, 14–17 October 2012; pp. 2721–2727.
41. Chowdhary, A.; Pisharody, S.; Alshamrani, A.; Huang, D. Dynamic game based security framework in SDN-enabled cloud networking environments. In Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, Scottsdale, AZ, USA, 24 March 2017; pp. 53–58.

42. The Software that Empowers Network Professionals. Available online: https://gns3.com (accessed on 15 November 2022).
43. OMNeT++ 6.0. Available online: https://omnetpp.org (accessed on 15 November 2022).
44. NS-3 Network Simulator. Available online: https://www.nsnam.org (accessed on 15 November 2022).
45. Virtual PC Simulator. SourceForge. Available online: https://sourceforge.net/projects/vpcs/?source=directory (accessed on 15 November 2022).
46. Parrot Security Os. Available online: https://www.parrotsec.org (accessed on 15 November 2022).
47. Nmap. Available online: https://nmap.org (accessed on 15 November 2022).
48. Wang, C.N.; Yang, F.C.; Vo, N.T.; Nguyen, V.T.T. Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs. *Drones* **2022**, *6*, 363. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.