ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.054:004.056.53 **doi: 10.32620/reks.2026.1.18**

Artem ABAKUMOV[1], Vyacheslav KHARCHENKO[1], Peter POPOV[2]

[1] ***National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine***
[2] ***City St George's, University of London, London, United Kingdom***

PROACTIVE UNMANNED AERIAL SYSTEMS CYBERSECURITY ANALYSIS: COMBINING A PRIORI – A POSTERIORI IMECA AND PENETRATION TESTING METHODS

*The **subject** of this study is the proactive cybersecurity analysis process of Unmanned Aerial Systems (UAS). The **goal** of this study is to reduce cybersecurity risks in UAS operations by developing a proactive analysis method that combines systematic risk identification with empirical validation in a controlled environment. The **objectives** of the study are: (a) to justify the usefulness of proactive cybersecurity analysis for UAS, (b) to develop a corresponding method, (c) to experimentally demonstrate the usefulness and applicability of the proposed method experimentally, and (d) to derive and assess a list of recommended countermeasures. The **methods** used in the study include Intrusion Modes and Effects Criticality Analysis (IMECA) and penetration testing. The **results** of the study are as follows: (a) a staged method for proactive UAS cybersecurity analysis was developed, combining a priori assessment, controlled reproduction of selected intrusion scenarios, and a posteriori refinement of risk estimates; (b) a block diagram of proactive UAS cybersecurity analysis was developed to formalize the vulnerability identification and assessment process; (c) a SITL platform deployed on a workstation running Kali Linux was used for reconnaissance, vulnerability and misconfiguration scanning, and intrusion mode simulation; (d) preliminary identified intrusion modes were experimentally confirmed, which led to the discovery of 35 additional intrusion modes linked to a common initial access vulnerability in the Wi-Fi protocol, four of which fell into the unacceptable risk zone; (e) a priori and a posteriori IMECA tables and criticality matrices were constructed; and (f) recommended countermeasures were derived and assessed. The **conclusions** of the study are as follows: (a) the proposed method enables systematic identification of intrusion modes and empirical refinement of probability, severity, and risk estimates; (b) the scientific novelty lies in integrating the IMECA method with a priori prediction and a posteriori refinement based on observations from UAS penetration testing procedures; (c) the developed block diagram proved useful for formalizing vulnerability detection and minimizing uncertainty in risk assessment; (d) the proposed method's usefulness and applicability were demonstrated on the SITL platform; and (e) no intrusion mode remains in the unacceptable risk zone following the potential implementation of the recommended countermeasures; three Wi-Fi-dependent modes retain a residual risk whose complete elimination requires an architectural rather than a configuration-level decision.*

Keywords: *Unmanned Aerial Systems; cybersecurity; IMECA; penetration testing; vulnerabilities; intrusion modes.*

1. Introduction

1.1. Motivation

Recently, the role of Unmanned Aerial Systems (UASs) has undergone a transformation from targeted use in counterterrorism operations to deep integration into full-scale combat operations. The use of UASs allows missions to be carried out more effectively, minimizing personnel risks and reducing civilian casualties. Modern unmanned platforms have evolved from reconnaissance tools into multifunctional platforms capable of providing fire support and delivering precision strikes [1].

Commercial off-the-shelf (COTS) UASs have become particularly important under the conditions of Russia's full-scale military invasion of Ukraine [2]. Although these devices demonstrate high cost-effectiveness, they contain critical vulnerabilities that are unacceptable for sensitive missions. Manufacturers' built-in protocols broadcast unencrypted location data about an operator, turning the control station into a target [3].

Consequently, deep software adaptation is required for COTS UASs to avoid deanonymization and remove flight zone restrictions. However, manufacturers constantly update factory firmware, rendering pre-customized versions incompatible with the latest UAS models [4].

The dominance of electronic warfare capabilities, which account for up to 90% of COTS UAS losses in intense combat, further complicates the current situation. Since COTS UASs often operate on unprotected

frequencies, leaving them vulnerable to jamming and spoofing attacks, there is an urgent need to modify the software of communication and navigation modules [5]. Given the UAV loss rate running into the thousands of units per month, relying solely on reactive defence methods is insufficient [6].

A shift to systematic cybersecurity analysis, which involves proactively identifying vulnerabilities (including zero-day vulnerabilities) in firmware, communication channels, and other critical UAS components, is necessary [7]. It is the only approach that minimizes the risks of interception, loss of control, or position disclosure. Moreover, firmware modifications can introduce previously unknown vulnerabilities, even though they address the tactical problem of masking. Systematic cybersecurity analysis allows us to verify whether the custom firmware has made the UAS even more vulnerable than it was before the modification. Furthermore, the cost of systematic cybersecurity analysis in laboratory conditions is significantly lower than the costs associated with mission failure or critical asset and personnel loss.

1.2. State of the art

Recent academic studies indicate that the field of UAS cybersecurity analysis is developing in several interrelated directions.

The first research area focuses on the systematic analysis and quantitative assessment of vulnerabilities and on threat modelling based on the adaptation of traditional approaches, such as CVSS and STRIDE, as well as the development of specific assessment metrics for UAVs. While STRIDE is widely used for threat categorization, it often overlooks the operating environment's trust level. To address this, [8] proposed xT-STRIDE, a modification that introduces the concept of trust levels. The results of modelling using a Petri net demonstrated that considering trust levels reduces the number of threats requiring active mitigation from 120 to 40, focusing limited UAV resources on threats relevant to the specific operational context and trust level. [9] formalized the application of STRIDE to UAS network layers and control systems, proposing a pseudocode for automated threat detection. Among specialized solutions, the value of the approach proposed in [10], which introduced its own quantitative assessment system, namely, the Drone Security Scoring System (D3S), is worth emphasizing. The assessment was conducted on a scale from 0 to 5 based on the analysis of UAV characteristics, communications, software, and vulnerability to common cyberattacks.

The second area focuses on adapting functional safety approaches, such as Failure Modes, Effects, and Criticality Analysis (FMECA), to the cybersecurity domain. The Intrusion Modes and Effects Criticality Analysis (IMECA) method is central to this approach. In [11], the authors pioneered the adaptation of FMECA for the Internet of Drones (IoD), creating a method for assessing the criticality of cyber intrusions that considers not only the presence of a breach but also its impact on system reliability. The authors of [12] made a significant contribution to the development of this area by proposing the use of IMECA for multifunctional UAV fleets under combined cyberattacks. The researchers developed basic models of sequential, parallel, and sequential-parallel intrusion chains, which enabled the calculation of changes in the probability and severity of effects when implementing complex cyberattack chains that cannot be correctly evaluated during isolated analysis. IMECA is a powerful method for assessing UAS cybersecurity, but it relies on expert assessments.

The third area involves analyzing UAS cybersecurity through experimental procedures such as penetration testing. In [13], the authors developed the Drone Attack Tool (DRAT), which facilitates attacks on Wi-Fi, but requires manual adaptation to other UAV models that are outside the scope of that study. Additionally, DRAT has limited functionality against secure protocols. [10] integrated penetration testing approaches into the cybersecurity analysis of common COTS UAVs and reproduced a few known cyberattacks, including de-authentication, flooding, and replay attacks. [14] emphasized the critical role of advanced penetration testing techniques, which are often ignored in theoretical models. [15] presented the Interceptor for Neutralization and Drone Remote Access (INDRA) cloud platform, which implements the concept of remote penetration testing. Unlike local tools, INDRA uses a client-server architecture where the attacking module can be placed on a UAV interceptor, allowing for de-authentication and GPS spoofing, which are centrally controlled via a cloud interface. The reviewed studies in the field of penetration testing are mostly limited to reproducing cyberattacks on COTS UAV/UAS platforms with low cybersecurity levels, and the criterion for experimental success is a binary assessment of success/failure, without an in-depth analysis of the cyber-physical effects of UAS hacking.

Based on the analysis of academic studies in the three mentioned research areas, it can be concluded that although the existing approaches are interconnected, they are often advanced without sufficient consideration of the feasibility and integration possibilities. Theoretical models lack comprehensive empirical support, whereas studies based solely on practical testing focus on exploiting vulnerabilities and replicating cyberattacks without assessing the effects and risks and do not consider the possibility of parallel/sequential intrusion combinations.

Therefore, a comprehensive, proactive approach that combines the assessment of cyber threats and UAS vulnerabilities with the validation of these assessments through the integration of experimental procedures

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

is urgently needed. In addition, it is important not only to confirm or refute the existence of vulnerabilities and to simulate intrusion modes but also to assess the cyber-physical effects and identify countermeasures to mitigate them.

1.3. Objectives

The subject of the study is the proactive cybersecurity analysis process of UAS. The goal of this study is to reduce the cyber risks of UAS operations by developing a proactive analysis method that combines systematic risk identification with empirical validation in a controlled environment.

The objectives of the study are as follows:

- justify the usefulness of proactive cybersecurity analysis for UAS;
- develop a corresponding method;
- to demonstrate the applicability and usefulness of the proposed method;
- to derive and assess a list of recommended countermeasures.

To achieve this goal, the study will follow a staged research approach. Relevant threats, vulnerabilities, and potential intrusion modes will be preliminarily identified and assessed. Next, the selected scenarios will be reproduced in a controlled environment to evaluate their feasibility and cyber-physical consequences. Finally, the obtained results will be used to refine risk estimates and support the selection of recommended countermeasures.

The paper is structured as follows: Section 2 presents the proposed method for proactive UAS cybersecurity analysis; Section 3 describes its experimental verification on a UAS simulation platform; Section 4 discusses the obtained results and limitations; and Section 5 presents the conclusions and outlines directions for further research.

2. Proactive UAS cybersecurity analysis method

The proposed method is intended to be applied before operational deployment and before the occurrence of actual intrusions. Rather than reacting to an observed intrusion, the proposed method anticipates possible intrusion modes, estimates their cyber-physical effects, and validates these estimates in a controlled experimental environment. This is particularly relevant for UASs, where firmware modification, delayed security patch incorporation, and supporting component vulnerabilities may create mission-relevant cybersecurity risks.

To address these issues, the method combines IMECA with experimental penetration testing, in which IMECA provides a systematic, expert-driven basis for identifying potential intrusion modes and for the preliminary assessment of their probability, severity, risk level, and effects on UAS missions. Penetration testing complements this analysis by reproducing selected intrusion modes and observing the actual behaviour of the UAS under controlled conditions. In this way, IMECA guides the selection of prior intrusion modes, while penetration testing provides empirical evidence for confirming, rejecting, or refining the initial IMECA assumptions.

The method is implemented as a sequential three-stage procedure. The terms “a priori” and “a posteriori” are used in their general epistemological sense: “a priori” denotes an assessment performed before empirical observations, whereas “a posteriori” denotes an assessment refined after such observations.

The three stages are:

- a priori IMECA, which provides an initial forecast of the effects and criticality scores of potential intrusion modes; and
- intrusion mode simulation through penetration testing, which is used to reveal known and hidden vulnerabilities and verify the assumptions of the a priori IMECA;
- a posteriori IMECA refines the estimated probability of successful exploitation and the severity of cyber-physical effects for each confirmed intrusion mode.

IMECA is a semi-formal tabular risk-based method of cybersecurity analysis. It constructs a matrix assessing probability, severity, and criticality, and analyzes the effects of countermeasures [11, 12]. The key idea of the method is to analyze interrelated chains in stages:

$$\text{threat} \rightarrow \text{vulnerability} \rightarrow \text{intrusion mode} \rightarrow \rightarrow \text{effects evaluation} \rightarrow \text{countermeasures selection}$$

A threat is understood as a potential cause of an undesirable incident that could damage the system or its environment. Threats to the IMECA originate from external intruders or internal violators who aim to compromise the confidentiality, integrity, and availability (CIA) of the UAS to disrupt its mission.

A vulnerability is a weakness in software, hardware, data transmission protocols, or UAS configuration that a threat actor can exploit to compromise the system’s CIA properties. The presence of a vulnerability is a prerequisite for a successful intrusion (i.e., vulnerability exploit).

The intrusion mode is a key element describing the specific technical way in which a threat exploits a vulnerability to penetrate a system or disrupt its functioning [11, 12].

The identified effects are classified according to their effect on the UAS mission (loss of control, video stream leakage, physical destruction, operator disorientation, etc.) and CIA violations.

Criticality assessment within the IMECA is based on three interrelated parameters [12]:

- Probability (P) characterizes the likelihood of a specific attack being carried out through an existing vulnerability, considering the attacker's capabilities and the intrusion chain's complexity. At the a priori stage, single-step or direct attacks are rated High, attacks requiring 2-3 consecutive steps are rated Medium, and attacks requiring 4 or more steps are rated Low. At the a posteriori stage, P is adjusted based on the results of the intrusion mode simulation.
- Severity (S) reflects the scale of negative consequences for the UAV and the operator, including the impact on confidentiality, integrity, and availability, as well as the degree of threat to mission execution. Complete mission termination or a threat to the operator's physical safety corresponds to High; partial degradation of system functions corresponds to Medium; and minor operational impact corresponds to Low. At the posteriori stage, S is calibrated based on the observed cyber-physical consequences.
- Risk (R) is a comprehensive indicator that integrates both parameters and characterizes the overall degree of potential intrusion impact on the system.

According to [12], the Probability (P) and Severity (S) metrics are measured on a 10-point ordinal scale, where a value of 1 corresponds to the minimum level and a value of 10 corresponds to the maximum level. This study proposes to linearly normalize both indicators to the unit interval (0, 1] to ensure a probabilistic interpretation of P and uniform comparability of assessment scores:

$$P_{norm} = \frac{P}{P_{max}} = \frac{P}{10}, \quad (1)$$

$$S_{norm} = \frac{S}{S_{max}} = \frac{S}{10}, \quad (2)$$

$$P_{norm}, S_{norm} \in (0, 1], \quad (3)$$

In formulas (1) - (3), P and S denote the original scale values, and P_{norm} and S_{norm} denote their normalized counterparts, respectively. In this context, Pnorm allows for a probabilistic interpretation as a relative measure of the likelihood of a successful intrusion, whereas S_{norm} is a normalized relative measure of the UAS mission's consequences' severity.

A single system of linguistic levels with uniform intervals is defined for both parameters, as shown in formula (4), where x denotes either P_{norm} or S_{norm}:

$$\ell(x) = \begin{cases} \text{Low}, & x \in (0, 0.3] \\ \text{Medium}, & x \in (0.3, 0.7], \\ \text{High}, & x \in (0.7, 1.0] \end{cases} \quad (4)$$

A three-zone risk classification is used to interpret the results [12]. The risk zone is determined using a correspondence table in which each combination of linguistic levels P and S is mapped to the corresponding zone.

For brevity, P_{norm} and S_{norm} are referred to as P and S throughout the remainder of this paper. The value of R for each intrusion mode is determined by mapping the corresponding P and S linguistic levels to the corresponding risk zone.

Next, at the stage of selecting countermeasures for each intrusion mode, protective mechanisms are proposed. Implementing countermeasures aims to reduce risks. An example of how to complete the IMECA table is presented in Table 1.

A criticality matrix is constructed to support decisions on countermeasure implementation (Table 2). Intrusion modes in the unacceptable (red) risk zone require mandatory countermeasures because they may lead to mission failure or operator safety. Countermeasures are desirable but not critical for intrusion modes in the acceptable (yellow) or controlled (green) risk zones, and the risk may be accepted as residual.

Table 1

IMECA table example

№	Threat	Vulnerability	Intrusion Mode	Effect	Criticality			Countermeasures
					P	S	R	
1	Threat actor	Weakness in the system that could lead to an intrusion	Exploitation method or cyberattack type	Effects of a successful intrusion	Low - High	Low - High	Low - High	Recommended protective measures to reduce risk

Table 2

IMECA criticality matrix example

Probability \ Severity	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Next, Figure 1 shows a block diagram of the algorithm that integrates key penetration testing processes (i.e., information gathering, scanning and intrusion mode simulation) between the priori and a posterior IMECA. The input data comprises the examined system architecture, preliminary vulnerability scanning results, and threat and vulnerability database data. The result of this stage is an a priori IMECA table in which experts construct interrelated "threat–effect" chains and assign preliminary criticality scores.

The countermeasure selection stage following the a priori analysis was removed to reduce the time consumption.

Subsequently, a validation procedure is performed for each defined chain by simulating the intrusion mode in a controlled environment. During this process, related threats and vulnerabilities are also revealed.

The next step is to verify the intrusion's success. If the intrusion is unsuccessful or impossible because of the specifics of the UAS architecture, the probability score decreases; if successful, it increases.

Next, a reanalysis of the effects, comparison with previous estimates, and severity calibration are performed. The verification results are used to update the criticality matrix. The cycle is repeated until each chain has been examined.

The algorithm produces a posteriori IMECA table and criticality matrices, which are used to select countermeasures in accordance with acceptable risk criteria.

3. Experimental verification of the method

3.1. Limitations

Given the current martial law conditions in Ukraine, the lack of safe areas for field testing, limited access to specialized hardware required for full-scale experiments, and the risk of physical damage to the UAS during testing, experimental verification of the developed methodology for proactive UAS cybersecurity analysis was experimentally verified in a simulation environment.

This decision enabled the reproduction of intrusion scenarios under controlled, repeatable conditions, the observation of their cyber-physical effects without endangering personnel or equipment, and the avoidance of operational and logistical constraints associated with real-world testing.

Therefore, the simulation environment was selected as a safe and practical alternative for the initial validation of the proposed method.

3.2. Simulation environment setup

A key requirement of the verification process is to create the necessary conditions for emulating UAS intrusion scenarios. Based on an analysis of existing solutions [16], the Damn Vulnerable Drone (DVD) simulation platform [17] was selected for the following reasons:

- it uses the Software-in-the-Loop (SITL) principle, which ensures that the detected vulnerabilities and system components' response to intrusions are identical to the actual behaviour of the real UAS;
- the simulation platform architecture contains common vulnerabilities in the technologies used (e.g., MAVLink, ArduPilot, WPA2, etc.);
- The platform is distributed under the MIT license, making it available for scientific research.

The simulation platform is deployed on a local workstation running the Kali Linux operating system. As shown in Figure 2, its architecture consists of five key components [17]:

- Flight Controller (FC). It runs on ArduPilot firmware, simulating UAV flight control processes. Interaction with the simulation environment occurs through the Gazebo interface, which allows process virtual sensor data and responding to changes in the environment as a physical device would;
- Companion Computer (CC). It is an integrated module that performs high-level computing tasks that exceed the flight controller's resource capabilities. Its functions include managing wireless interfaces, maintaining telemetry logs, providing streaming video data for reconnaissance, and interacting with autonomous navigation systems;
- Ground Control Station (GCS). It serves as an operator interface, providing mission planning, mapping, video stream viewing, and manual control via the manipulator. Data exchange with the flight controller and host computer is conducted via a simulated wireless channel using the MAVLink protocol;
- Simulation environment (Gazebo). It provides a detailed three-dimensional space visualization and physically accurate modelling of flight aerodynamics. The component is responsible for the realistic response of the UAV model to control commands and the influence of external environmental factors;
- QGroundControl. It is a software used for planning flight missions, configuring UAV parameters, monitoring telemetry in real time, and post-flight data analysis. The toolkit allows creation of flight paths.

The verification process combines practical and analytical parts. The practical part, carried out on the simulation platform, includes reconnaissance and scanning activities, intrusion mode identification, and real-time simulation. The analytical part comprises the construction of a priori and a posteriori IMECA tables and criticality matrices.

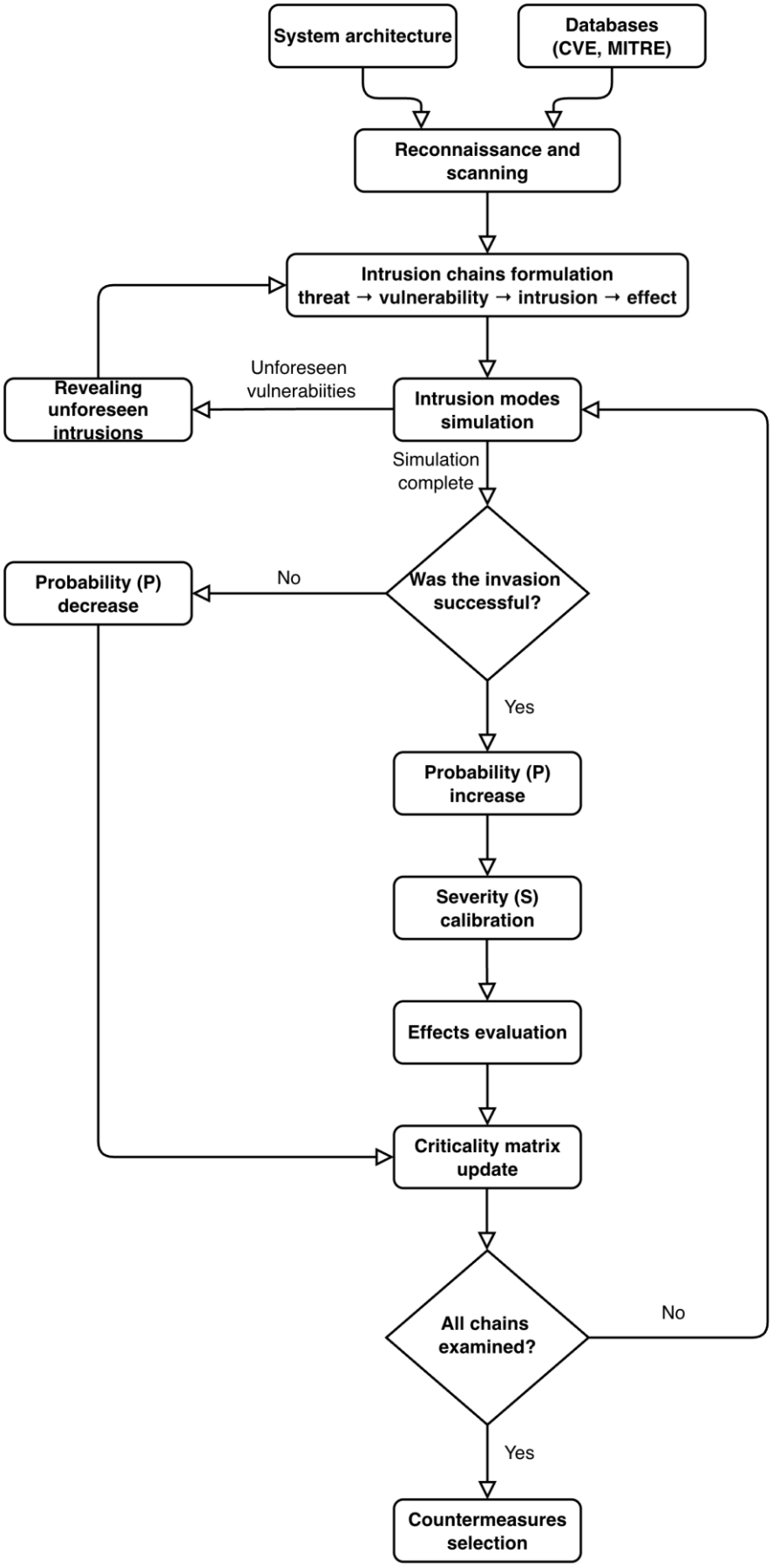

Fig. 1. Block diagram of proactive cybersecurity analysis

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

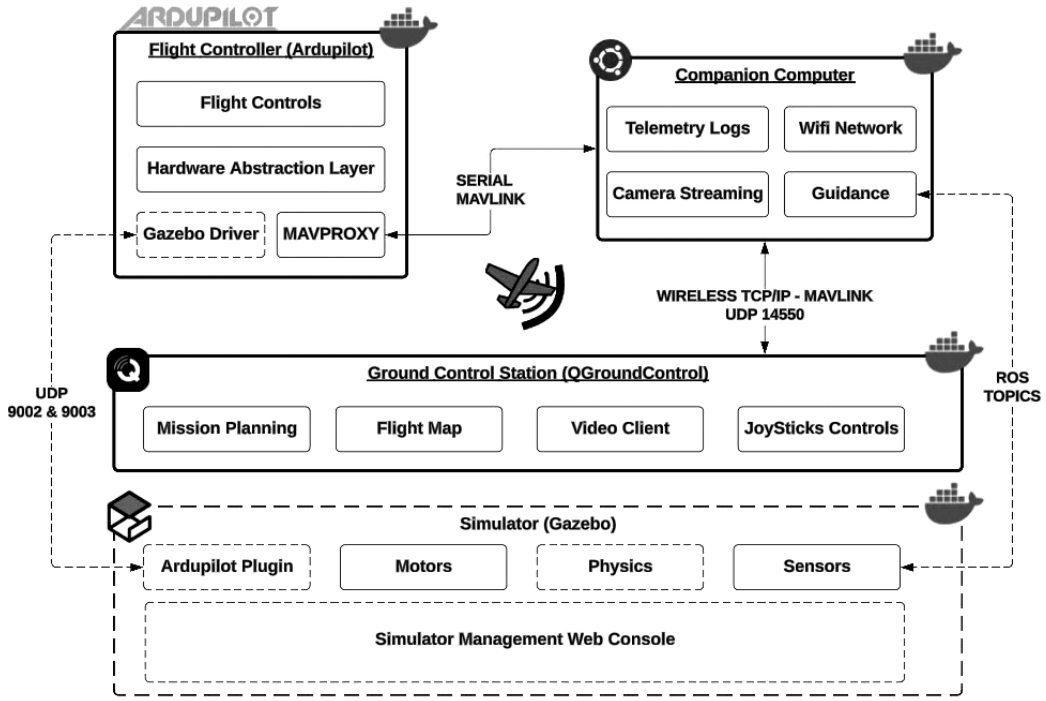

Fig. 2. High-level simulation platform architecture [17]

3.3. Reconnaissance and scanning techniques

At the initial reconnaissance stage, the intruder station's wireless adapter was set to monitor mode, and airodump-ng was used to scan the Wi-Fi spectrum. As shown in Figure 3, the scan identified the target access point, Drone_Wifi, and revealed the following network security parameters: WPA2 encryption type, PSK authentication method, and channel 6 operation. Another key finding was an active client with the MAC address 02:00:00:00:02:00 exchanging data with the UAV. This reconnaissance and scanning results provide the basis for further detailed modelling of Drone_Wifi network intrusion scenarios.

3.4. A priori IMECA

Based on the analysis of the preliminary reconnaissance results, two critical and interrelated intrusion modes were added to the a priori IMECA table (Table 3):

- Dictionary attack – a password-cracking method in which the attacker attempts authentication using a predefined list of passwords or leaked credentials [9].
- Wi-Fi deauthentication – an attack that forges deauthentication frames to disconnect a client from the access point and disrupt the communication link [10, 13].

This choice is due to the detected configuration. The use of the WPA2 standard without Management Frame Protection (MFP) enabled, combined with the presence of an active client, makes the system vulnerable to a Wi-Fi deauthentication attack. Reproducing this intrusion mode allows the intruder to disrupt the control channel's availability and force the client to reconnect.

However, if a 4-way handshake is intercepted, the PSK authentication mechanism is vulnerable to dictionary attacks. Wi-Fi deauthentication enables rapid handshake interception in the active mode. Password compromise is also possible through passive monitoring of the airwaves until the operator initiates a legitimate connection. In this scenario, an intruder can gain access to the Drone_Wifi network without being detected.

Accordingly, a dictionary attack can be classified as either a passive isolated intrusion mode or an active combined sequential intrusion mode. This variability is considered when the probability is evaluated. The passive intrusion mode is technically simpler but has a lower success rate because it depends on external factors beyond the control of the intruder. On the other hand, the active intrusion mode requires a prior Wi-Fi deauthentication attack. In both cases, the physical presence of the intruder within the range of the Drone_Wifi network is a critical condition for the implementation.

The probability (P) score for Wi-Fi deauthentication was assessed as “High” (H) and as “Medium” (M) for the dictionary attack. The IMECA table structure has been extended by adding the intrusion chain column to visualize the dependencies between intrusion modes.

The Severity (S) score for Wi-Fi deauthentication is set to “High” (H) because this intrusion mode disrupts the availability of the control channel. A loss of communication between the GCS and the UAV is a critical incident

```
CH  6 ][ Elapsed: 6 s ][ 2026-01-18 11:28

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

02:00:00:00:01:00  -28   0       79       913  111   6  130   WPA2 CCMP   PSK  Drone_Wifi

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

02:00:00:00:01:00  02:00:00:00:03:00  -29    0 - 1e     0        1
02:00:00:00:01:00  02:00:00:00:02:00  -29   11e-11e     0      913
```

Fig. 3. Network scanning results

Table 3

A priori IMECA table

№	Threat	Vulnerability	Intrusion Mode	Intrusion Chain	Effect	Criticality		
						P	S	R
1	External intruder	No MFP	Wi-Fi deauthentication	active: ID1	Flight mission termination (A)	H	H	H
2		Weak password	Dictionary attack	passive: ID1 active: ID1 → ID2	Unauthorized access (C, I)	M	H	H

Table 4

A priori criticality matrix

Probability \ Severity	Low	Medium	High
Low			
Medium			2
High			1

that leads to the forced suspension of the flight mission in the context of a UAS operation.

The Severity (S) score for the dictionary attack is also set to “High” (H), as successful cracking of the Wi-Fi password results in complete compromise of confidentiality and integrity.

Based on the evaluation results, both intrusion modes are classified as belonging to the critical risk zone in the criticality matrix (Table 4).

3.5. Simulation of intrusion modes

According to the developed tree of potential intrusion modes shown in Figure 4, the initial stage of the active scenario for gaining access to the UAS wireless network is the execution of a Wi-Fi deauthentication attack.

The aireplay-ng utility was used to implement this in practice. An aireplay-ng command was executed to initiate the sending of targeted deauthentication frames to the GCS address on behalf of a legitimate access point. Figure 5 shows the result of the Wi-Fi deauthentication attack.

Simultaneously, background monitoring with airodump-ng recorded the transmission of EAPOL frames. The successful interception of the cryptographic handshake is confirmed by the message “WPA handshake: 02:00:00:00:01:00” in the upper right corner of the terminal (Figure 6). The obtained data were automatically saved to the capture_wpa-01.cap file.

The next step is to execute a dictionary attack. Since the intercepted hash is contained in the received file, the attack was conducted offline. To retrieve the password, the aircrack-ng utility with the rockyou.txt dictionary was used. Figure 7 shows the result of executing the command. The access key was found in less than a second due to the password's low entropy, confirming the criticality of the weak password vulnerability.

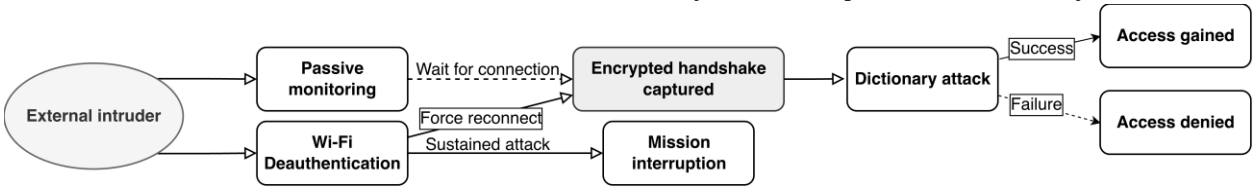

Fig. 4. Potential intrusion modes tree

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

```
└─$ sudo aireplay-ng --deauth 10 -a 02:00:00:00:01:00 -c 02:00:00:00:02:00 wlan0mon
11:34:11  Waiting for beacon frame (BSSID: 02:00:00:00:01:00) on channel 6
11:34:11  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:12  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:12  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:13  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:14  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:14  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:15  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:15  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:16  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:16  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
```

Fig. 5. Wi-Fi deauthentication attack execution

```
CH  6 ][ Elapsed: 18 s ][ 2026-01-18 11:34 ][ WPA handshake: 02:00:00:00:01:00

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

02:00:00:00:01:00  -28   0      215     1583  111   6  130   WPA2 CCMP   PSK  Drone_Wifi

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

02:00:00:00:01:00  02:00:00:00:03:00  -29    0 - 1e     0        1
02:00:00:00:01:00  02:00:00:00:02:00  -29    1e- 1e     0     2865  EAPOL
```

Fig. 6. 4-way handshake interception

```
                          Aircrack-ng 1.7

[00:00:00] 91/10303727 keys tested (1153.96 k/s)

Time left: 2 hours, 28 minutes, 48 seconds                 0.00%

                      KEY FOUND! [ 1234567890 ]


Master Key     : B0 8A 11 70 58 2C 5E 6E D8 41 D2 F2 07 CE C3 F8
                 2A C0 17 16 02 32 6F 73 48 F8 9F AE EE B4 73 8F

Transient Key  : E4 B9 3B 3E 54 F0 60 47 E1 E8 6E 56 62 48 F0 42
                 88 8C 0B D7 CD F0 93 5D 0B 6E 22 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : CB 36 A9 8E F8 C9 12 18 81 97 60 77 7D B2 03 C6
```

Fig. 7. Dictionary attack execution result

The last step was to connect to the Drone_Wifi network using the credentials obtained. After the connection, the network parameters were checked. The "ip a" command showed that the wlan0 interface had successfully obtained the IP address 192.168.13.11/24. This indicates that the intruder is on the same subnet as the GCS. Finally, the availability of the UAV host (192.168.13.1) was checked using the ping utility to confirm control over the communication channel, and packet exchange was successful, confirming access to the UAS network. Figure 8 shows the resulting intrusion tree.

Gaining access to the Drone_WiFi network allows external intruders to conduct further reconnaissance and deeper intrusions while acting as internal violators, which can be classified as combined if considered separately.

Further exploration involved the use of:

- reconnaissance and scanning tool (Nmap),
- traffic interception and analysis tools (Wireshark, Ettercap),
- MAVLink protocol manipulation tools (Pymavlink, MAVProxy),
- authentication auditing tool (Hydra).

ARP spoofing was exploited at the internal network level to enable passive monitoring and interception of unencrypted data streams, including video streaming and telemetry.

The bulk of further intrusions focused on exploiting vulnerabilities in the MAVLink protocol. Injection and spoofing attacks were successfully executed due to the lack of packet authentication mechanisms. This allowed for the manipulation of navigation sensor readings, the substitution of system statuses presented to the operator, and the injection of unauthorized control commands, up to and including complete takeover of mission control and flight mission termination.

Additionally, the resilience of companion computer services was examined, revealing vulnerabilities to unauthorized access through open APIs, weak administrative interface passwords, and unprotected file transfer protocols. Figure 9 shows the resulting intrusion mode tree.

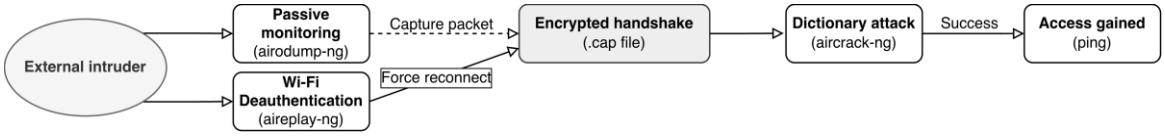

Fig. 8. Dictionary attack tree

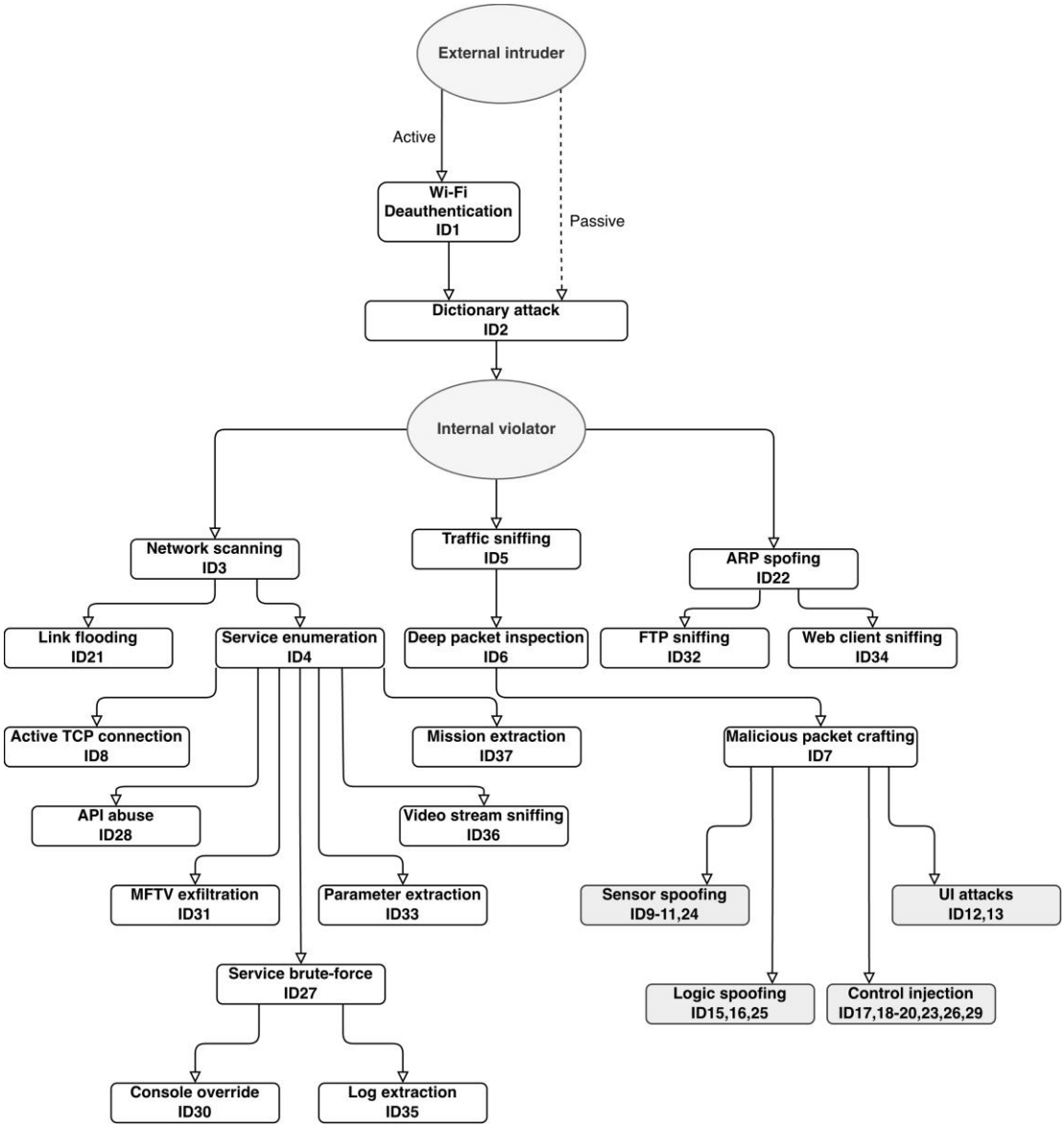

Fig. 9. Resulting intrusion modes tree

3.6. A posteriori IMECA

Following a series of intrusions into the simulation platform configuration, Tables 5 and 6 present an a posteriori IMECA table and criticality matrix. The added sequential modes differ in the length of the intrusion chain, ranging from 2 to 5 stages, with the probability decreasing as the chain length increases. To highlight the affected components, the IMECA table structure was extended with a "Component" column with the following possible values: internal network (INW), companion computer (CC), flight controller (FC), GCS, telemetry (TL), and communication link (CL).

The recommended countermeasures were selected based on an analysis of the NIST SP 800 series guidelines [18], the ISO/IEC 27002:2022 standard [19], technical documentation for MAVLink protocols [20] and ArduPilot [21], and OWASP recommendations [22]. The selection was guided by three criteria. The first is that each countermeasure must address a specific vulnerability; the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

second is implementability within the target architecture; and the third is the priority of reducing the probability of successful exploitation over limiting the severity of consequences, since reducing the likelihood of intrusion prevents the entire downstream chain of dependent intrusion modes. Where a single countermeasure was insufficient, a pair of countermeasures was selected in accordance with the defence-in-depth principle. Table 7 presents the resulting criticality matrix following countermeasure implementation.

Table 5

A posteriori IMECA table

№	Threat	Vulnerability	Intrusion Mode	Intrusion Chain	Component	Effect	Criticality			Countermeasures
							P	S	R	
1	External intruder	No MFP	Wi-Fi deauthentication	active: ID1	CL	Flight mission termination (A)	H	H	H	1. Enable 802.11w MFP. 2. Frequency-hopping spread spectrum.
2		Weak password	Dictionary attack	passive: ID1 active: ID1→ ID2	CL	Unauthorized access (C, I)	H	H	H	1. Strong password policy. 2. Switch to WPA3 encryption standard.
3	Internal violator	No network segmentation	Network scanning	active: ID2→ID3	INW	Network topology disclosure (C)	M	M	M	1. VLAN network isolation. 2. Wireless client isolation.
4		Open network ports	Service enumeration	active: ID2→ID3→ ID4	CC	Identification of vulnerable services (C)	M	M	M	1. Disable unused services. 2. Port knocking.
5		Predictable sequence number	Traffic sniffing	passive: ID2→ID5	TL	Real-time telemetry leak (C)	M	H	H	1. VPN tunnelling. 2. AES-256 data encryption.
6		Predictable sequence number	Deep packet inspection	passive: ID2→ID5→ ID6	TL	Protocol analysis (C)	M	M	M	1. MAVLink v2 packet signing. 2. System ID randomization.
7		Improper input validation	Malicious packet crafting	active: ID2→ID5→ID6→ ID7	FC	Creation of a valid package (I)	L	H	M	1. Strict packet parsing and validation. 2. Cyclic redundancy check validation.
8		No TCP authentication	Active TCP connection	active: ID2→ID3→ID4→ID8	FC	Telemetry port access (C)	L	H	M	1. Mutual TLS authentication. 2. IP address whitelisting.
9	Internal violator	No integrity check	Attitude data spoofing	active: ID2→ID5→ ID6→ ID7→ID9	FC	GCS disorientation (I)	L	H	M	1. MAVLink packet signing. 2. IMU sensor priority logic.
10		Improper Failsafe Logic	Battery spoofing	active: ID2→ID5→ ID6→ ID7→ID10	FC	Forced emergency RTH (A)	L	H	M	1. Failsafe logic filtering. 2. Sensor voting mechanisms.
11		Unverified data source	GPS coordinates spoofing	active: ID2→ID5→ ID6→ID7→ ID11	FC	Deviation from the flight route (I)	L	H	M	1. Extended Kalman filter gating. 2. Optical flow backup navigation.

Table 5 (continued)

№	Threat	Vulnerability	Intrusion Mode	Intrusion Chain	Component	Effect	Criticality			Countermeasures
							P	S	R	
12	Internal violator	Improper UI validation	Error message injection	active: ID2→ID5→ ID6→ID7→ ID12	GCS	Psychological pressure on the operator (I)	L	H	M	1. UI message filtering. 2. Message whitelisting.
13		No rate limit	Text message flood	active: ID2→ID5→ ID6→ID7→ ID13	GCS	Loss of situational awareness (A)	L	M	L	1. Rate limiting. 2. Message deduplication.
14		Insufficient signal quality check	Satellite count spoofing	active: ID2→ID5→ ID6→ID7→ ID14	FC	Loss of GPS flight modes (I)	L	H	M	1. Multi-sensor data fusion. 2. Signed data injection.
15		Lack of physics sanity check	HUD spoofing	active: ID2→ID5→ ID6→ID7→ ID15	GCS	Misleading the operation (I)	L	H	M	1. Physics sanity checks. 2. Trusted data sources.
16		Implicit trust in reported status	System status spoofing	active: ID2→ID5→ ID6→ID7→ ID16	FC	Simulation of system failures (I)	L	M	L	1. Internal health checks. 2. Voting logic algorithms.
17		Insecure parameters configuration	Geofence data injection	active: ID2→ID5→ ID6→ID7→ ID17	FC	Removing flight restrictions (I)	L	H	M	1. Parameter locking. 2. Command signing.
18		No authentication for configuration	GPS glitching	active: ID2 → ID5 → ID6 → ID7 → ID18	FC	Navigation filter failure (A)	L	H	M	1. Checksum validation. 2. Hard-coded critical params.
19		Missing authentication for critical functions	Flight termination command	active: ID2→ID5→ ID6→ID7→ ID19	FC	Physical destruction (A)	L	H	M	1. MAVLink packet signing. 2. Physical safety switch.
20		Race condition	Denial of takeoff	active: ID2→ID5→ ID6→ID7→ ID20	FC	Motor arming lockout (A)	L	H	M	1. Source filtering. 2. Link encryption.
21		Uncontrolled resource consumption	Link flooding	active: ID2→ID3→ ID21	CL	Loss of control and telemetry channel (A)	M	H	H	1. Rate limiting. 2. Quality of service implementation.
22		Lack of ARP validation	ARP spoofing	active: ID2→ID22	INW	Interception of internal traffic (C)	M	H	H	1. Static ARP entries. 2. VPN.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Table 5 (continued)

№	Threat	Vulnerability	Intrusion Mode	Intrusion Chain	Component	Effect	Criticality			Countermeasures
							P	S	R	
23	Internal violator	No component authorization	Gimbal control hijack	active: ID2→ID5→ ID6→ID7→ ID23	FC	Reconnaissance sabotage (I)	L	H	M	1. Component authorization. 2. Command signing.
24		Implicit Trust in External Data	GPS injection	active: ID2→ID5→ ID6→ID7→ ID24	FC	Conflict between navigation sensors (I)	L	H	M	1. Disable external GPS injection. 2. Authenticated input.
25		Logic error in navigation	Return-to-Home point hijack	active: ID2→ID5→ ID6→ID7→ ID25	FC	UAV theft (A)	L	H	M	1. Geofence validation. 2. Operator confirmation requirement.
26		No write authorization	Mission injection	active: ID2→ID5→ ID6→ID7→ ID26	FC	Execution of an unauthorized flight task (I)	L	H	M	1. Mission signing. 2. Visual plan check.
27		Weak password	Service brute-force	active: ID2→ID3→ ID4→ID27	CC	Gaining full administrative control (C,I)	L	H	M	1. Strong password policy. 2. Fail2Ban/Lockout mechanism.
28		Unprotected API endpoint	API abuse	active: ID2→ID3→ ID4→ID28	CC	Critical services stopped (A)	L	H	M	1. JWT authentication. 2. Disable debug interfaces.
29		No command authorization	Auto mode injection	active: ID2→ID5→ ID6→ID7→ ID29	FC	Manual control loss (A)	L	H	M	1. RC override priority. 2. Command signing.
30		Excessive privileges	Console override	active: ID2→ID3→ ID4→ID27→ ID30	FC	Interception of control via terminal (I)	L	H	M	1. TLS/SSH authentication. 2. Session auditing.
31		Broken access control	MAVFTP exfiltration	active: ID2→ID3→ ID4→ID31	FC	Sensitive files theft (C)	L	H	M	1. Disable MAVFTP service. 2. Read-Only access.
32		Cleartext protocols	FTP sniffing	passive: ID2→ID22→ ID32	INW	Passive files interception (I)	M	M	M	1. Use SFTP/SCP. 2. Operational security.
33		Information Disclosure	Parameter extraction	active: ID2→ID3→ ID4→ID33	FC	System configuration disclosure (C)	L	M	L	1. Access Control Lists (ACL). 2. Command signing.
34		Cleartext HTTP	Web client sniffing	passive: ID2→ID22→ ID34	INW	Theft of operator credentials (C)	M	H	H	1. Enforce HTTPS. 2. WPA3 Enterprise.

Table 5 (continued)

№	Threat	Vulnerability	Intrusion Mode	Intrusion Chain	Component	Effect	Criticality			Countermeasures
							P	S	R	
35	Internal violator	Insecure Direct Object References	Log extraction	active: ID2→ID3→ ID4→ID27→ ID35	CC	Flight logs reveal (C)	L	H	M	1. Data at rest encryption. 2. Secure data wipe.
36		No Authentication for RTSP	Video stream sniffing	active: ID2→ID3→ ID4→ID36	CC	Unauthorized viewing of real-time video stream (C)	L	H	M	1. RTSP encryption. 2. Digest authentication.
37		Missing read authorization	Mission extraction	active: ID2→ID3→ ID4→ID37	FC	Compromise of mission plan and target points (C)	L	H	M	1. Mission encryption. 2. Air gap transfer.

Table 6

A posteriori criticality matrix

Probability \ Severity	Low	Medium	High
Low		13,16,33	7-12,14,15, 17-20,23-31,35-37
Medium		3,4,6,32	5,21,22,34
High			1,2

Table 7

Criticality matrix after countermeasure implementation

Probability \ Severity	Low	Medium	High
Low	3, 4, 6, 13, 16, 17, 24, 29, 31–33, 35–37	7–12, 14, 15, 18–23, 25–28, 30, 34	1, 2, 5
Medium			
High			

4. Discussion

This study expands the cybersecurity analysis framework by integrating IMECA with penetration testing [23], covering threat identification, vulnerability analysis, expert risk assessment, and countermeasure selection across UAS components.

In the proposed method, the relationship between a priori IMECA and penetration testing is bidirectional: a priori IMECA determines the initial set of intrusion modes from information gathering results, whereas penetration testing verifies these assumptions, reveals additional vulnerabilities and subsequent intrusion modes, and reassesses the results using the a posteriori IMECA.

Two previously identified intrusion modes were confirmed during experimentation on the simulation platform, leading to the discovery of 35 additional intrusion modes linked to a common initial access vulnerability in the Wi-Fi protocol. This demonstrates that penetration testing can substantially expand the inventory of intrusion modes rather than merely confirm individual scenarios. The Severity scores of the confirmed modes remained unchanged from the a priori assessment because the observed cyber-physical consequences matched the initial expert estimates. Of the 35 new intrusion modes, 4 fell into the unacceptable risk zone despite the successful execution of the Wi-Fi deauthentication and dictionary attacks.

The analysis of selected countermeasures indicates that effective mitigation would require a combination of architectural, cryptographic, and administrative controls if such vulnerabilities and intrusion modes were detected

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

in a real UAS. Following the implementation of the countermeasure, no intrusion mode remains in the unacceptable risk zone. Most countermeasures reduce risk by lowering the probability of successful exploitation, thereby preventing the intrusion effect from being achieved altogether. A subset reduces severity by limiting the actual impact of a successfully executed attack at the system level. Three intrusion modes (ID 1, 2, and 5) retain a medium residual risk. Their severity remains high because the consequences of a theoretically successful attack are inherently critical and cannot be mitigated by software controls alone. The complete elimination of residual risk for these modes would require abandoning the Wi-Fi channel as a transport medium, which is an architectural rather than a configuration-level decision.

The main limitation of the proposed method is its reliance on expert judgment. Structured questionnaires or expert groups can reduce this limitation, although the latter requires a dedicated procedure for coordinating decisions and processing results [24].

5. Conclusions and recommendations for further research

The main contribution of this study is the development and experimental verification of a method for proactive UAS cybersecurity analysis. The scientific novelty lies in the integration of the IMECA method with a priori prediction and a posteriori refinement based on UAS penetration testing procedures. The developed block diagram shows its usefulness in formalizing the vulnerability detection process and minimizing risk assessment uncertainty. The proposed method's usefulness and applicability were demonstrated using the SITL platform. The recommended countermeasures were derived and assessed: following their implementation, no intrusion mode remains in the unacceptable risk zone, with three Wi-Fi-dependent modes retaining a residual risk that requires an architectural rather than a configuration-level solution. Promising areas for further research include the following:

- adapting the method for UAV fleets by extending sets of vulnerable communication components and anticipating cyberattacks, including various types of combined attacks [12];
- transferring experimental verification from a simulation environment to laboratory conditions using physical UAS models and hardware;
- tracing IMECA results to evaluate safety based on "Security-informed Safety" and "Safety-informed Security" principles [25, 26].
- applying Bayesian inference [27, 28] to derive calibrated numerical probabilities from the combination of expert a priori assessments and penetration testing observations; these calibrated probabilities would subsequently enable the analysis of a formal attack tree with quantitative probability propagation.
- exploring the potential integration of AI-driven tools, such as machine learning and LLMs [29] for adaptive threat identification and explainable AI for protocol anomaly classification [30], into the proposed method to reduce reliance on expert judgment and enhance the threat detection and criticality assessment automation.

Contributions of authors: conceptualization – **Artem Abakumov, Vyacheslav Kharchenko, Peter Popov**; methodology, formulation of tasks – **Artem Abakumov, Vyacheslav Kharchenko**; experimental verification, results analysis, visualization, writing, original draft preparation – **Artem Abakumov**; review and editing – **Vyacheslav Kharchenko, Peter Popov**.

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Author **Vyacheslav Kharchenko** is a member of the Editorial Board of this journal. He were not involved in the peer review, handling, or decision-making process for this manuscript.

Financing

This research was conducted without financial support.

Data Availability

The manuscript has no associated data.

Use of Artificial Intelligence

The DeepL tool was used for accurate text translation and synonym selection. The Grammarly tool was used for spelling and grammar checks.

All the authors have read and agreed to the published version of this manuscript.

References

1. Jeler, E. G. Military and civilian applications of UAV systems. *Proceedings of the International Scientific Conference "Strategies XXI". The Complex and Dynamic Nature of the Security Environment*, Bucharest, Romania, Carol I National Defence University Publishing House, 2019, vol. 1, pp. 379-386.

2. Brown, H. *The drone revolution: Lessons from Ukraine*. Riga, Latvian Institute of International Affairs, 2025. Available at: https://liia.lv/en/publications/the-drone-revolution-lessons-from-ukraine-1476 (accessed February 11, 2026).

3. Slusher, M. N. *Lessons from the Ukraine conflict: modern warfare in the age of autonomy, information, and resilience*. Washington, DC, Center for Strategic and International Studies (CSIS), 2025. Available

at: https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience (accessed February 11, 2026).

4. Cook, D. *The innovation of consumer drones on the battlefield: a trip around the world*. Special Operations Association of America, 2025. Available at: https://soaa.org/consumer-drones-battlefield (accessed February 11, 2026).

5. Millynia, D. E., Risdhianto, A., Duarte, E. P., & Almubaroq, H. Z. Operational security in modern warfare: lessons from the Ukraine-Russia conflict. *Formosa Journal of Multidisciplinary Research (FJMR)*, 2025, vol. 4, no. 4, pp. 1975-1990.

6. Momoh, Z. & Malumfashi, A. L. The strategic deployment of unmanned aerial vehicles in contemporary armed conflicts: a comparative study of the Russia-Ukraine and Israel-Gaza conflicts. *Kashere Journal of Politics and International Relations*, 2025, vol. 3, no. 4, pp. 202–213.

7. Ariante, G. & Del Core, G. Unmanned aircraft systems (UASs): current state, emerging technologies, and future trends. *Drones*, 2025, vol. 9, no. 1, article no. 59. DOI: 10.3390/drones9010059.

8. Yerden, A. U., Senol, S., Kara, M. & Dilibal, S. xT-STRIDE threat model for unmanned air vehicle security. *International Journal of Information Security*, 2025, vol. 24, article no. 169. DOI: 10.1007/s10207-025-01082-4.

9. Sharma, D. D. Cybersecurity issues in UAV control and network system: a systematic review. *In*: Amine, A. (ed.) *Cybersecurity - current trends and future prospects*. London, IntechOpen, 2024. DOI: 10.5772/intechopen.114175.

10. Branco, B., Silva, J. S. & Correia, M. D3S: a drone security scoring system. *Information*, 2024, vol. 15, no. 12, article no. 811. DOI: 10.3390/info15120811.

11. Torianyk, V., Kharchenko, V. & Zemlianko, H. IMECA based assessment of Internet of Drones systems cyber security considering radio frequency vulnerabilities. *Proceedings of the 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS'2021)*, Khmelnytskyi, Ukraine, CEUR-WS.org, 2021, vol. 2853, pp. 460–470.

12. Zemlianko, G., & Kharchenko, V. IMECA analysis of cybersecurity for multi-functional UAV fleets under combined attacks: basic models and countermeasure choice. *Measuring and Computing Devices in Technological Processes*, 2023, no. 4, pp. 225-233. DOI: 10.31891/2219-9365-2023-76-30.

13. Veerappan, C. S., Keong, P. L. K., Balachandran, V., & Fadilah, M. S. B. M. DRAT: A penetration testing framework for drones. *Proceedings of the 2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA)*, Chengdu, China, IEEE, 2021, pp. 498-503. DOI: 10.1109/ICIEA51954.2021.9516363.

14. Malik, S. Security of unmanned aerial vehicle systems through advanced penetration testing. *TechRxiv*, 2024. DOI: 10.36227/techrxiv.172296783.30458380/v1.

15. Devine, T. R., Cunningham, D. J., Hasselman, T. J. K., Hudson, A. A., Roland, A. M., Scott, J. A., Thompson, G. W., Yokum, L. G., & Zekonis, P. F. INDRA: A drone penetration testing platform for cybersecurity education. In: Arabnia, H. R., Deligiannidis, L., Amirian, S., Ghareh Mohammadi, F., & Shenavarmasouleh, F. (eds) *Foundations of Computer Science and Frontiers in Education: Computer Science and Computer Engineering. CSCE 2024. Communications in Computer and Information Science*, vol. 2261, Cham, Springer, pp. 235-251, 2025. DOI: 10.1007/978-3-031-85930-4_22.

16. Dimmig, C. A., Silano, G., McGuire, K., Gabellieri, C., Hönig, W., Moore, J., & Kobilarov, M. Survey of simulators for aerial robots: an overview and in-depth systematic comparisons [survey]. *IEEE Robotics & Automation Magazine*, 2025, vol. 32, no. 2, pp. 153-166. DOI: 10.1109/MRA.2024.3433171.

17. Aleks, N. Damn Vulnerable Drone (DVD). Available at: https://github.com/nicholasaleks/Damn-Vulnerable-Drone (accessed February 11, 2026).

18. National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Available at: https://csrc.nist.gov/publications/sp800 (accessed February 11, 2026).

19. *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls*. Geneva, ISO/IEC Publ., 2022. 154 p.

20. Dronecode Project. *MAVLink Guide.* Available at: https://mavlink.io/en/guide/ (accessed February 11, 2026).

21. ArduPilot Dev Team. *ArduPilot Dev Guide*. Available at: https://ardupilot.org/dev/docs/ (accessed February 11, 2026).

22. OWASP. *Application Security Verification Standard (ASVS).* Available at: https://owasp.org/www-project-application-security-verification-standard/ (accessed February 11, 2026).

23. Abakumov, A., Kharchenko, V., & Popov, P. A hybrid cybersecurity assessment framework for unmanned aircraft vehicles based on IMECA and penetration testing. *Proceedings of the 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Naples, Italy, IEEE, 2025, pp. 7-14. DOI: 10.1109/DSN-W65791.2025.00032.

24. Babeshko, I., Illiashenko, O., Kharchenko, V., & Leontiev, K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques. *Mathematics*, 2022, vol. 10, no. 13, article no. 2297. DOI: 10.3390/math10132297.

25. Ivasiuk, O., Kharchenko, V., & Zemlianko, H. From Security Informed Safety to Safety Informed Security: Methodology and Case for PLC-based I&C Assessment. *International Journal of Computing*, 2025, vol. 24, no. 3, pp. 603-610. DOI: 10.47839/ijc.24.3.4199.

26. Bloomfield, R. E., Bishop, P. G., Butler, E., & Stroud, R. Security-Informed Safety: Supporting Stakeholders with Codes of Practice. *Computer*, 2018, vol. 51, no. 8, pp. 60-65. DOI: 10.1109/MC.2018.3191260.

27. Popov, P. Dynamic Safety Assessment of

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Autonomous Vehicle Based on Multivariate Bayesian Inference (DyAVSA). *Journal of Reliable Intelligent Environments*, 2025, vol. 11, no. 3, article no. 14. DOI: 10.1007/s40860-025-00252-4.

28. Puliyski, A., & Serbezov, V. Approaches to cybersecurity in UAS in the SORA process: a systematic literature review of standards, probabilistic models, and AI integration. *Engineering Proceedings*, 2026, vol. 121, no. 1, article no. 17. DOI: 10.3390/engproc2025121017.

29. Yang, Z., Zhang, Y., Zeng, J., Yang, Y., Jia, Y., Song, H., Lv, T., Sun, Q., & An, J. AI-driven safety and security for UAVs: from machine learning to large language models. *Drones*, 2025, vol. 9, no. 6, article no. 392. DOI: 10.3390/drones9060392.

30. Sun, Q., Zeng, J., Dai, L., Hu, Y., & Tian, L. XAI-based framework for protocol anomaly classification and identification to 6G NTNs with drones. *Drones*, 2025, vol. 9, no. 5, article no. 324. DOI: 10.3390/drones9050324.

Received 14.10.2025, Received in revised form 06.01.2025
Accepted date 15.01.2026, Published date 22.01.2025

ПРОАКТИВНИЙ АНАЛІЗ КІБЕРБЕЗПЕКИ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ: ПОЄДНАННЯ МЕТОДІВ АПРІОРНОГО–АПОСТЕРІОРНОГО IMECA ТА ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

А. І. Абакумов, В. С. Харченко, П. Т. Попов

Предметом дослідження є процес проактивного аналізу кібербезпеки безпілотних авіаційних комплексів. **Метою** є зменшення кібербезпекових ризиків під час їх експлуатації шляхом розроблення методу проактивного аналізу, що поєднує систематичне виявлення ризиків з їх емпіричною валідацією в контрольованому середовищі. **Завдання дослідження**: (а) обґрунтувати корисність проактивного аналізу кібербезпеки безпілотних авіаційних комплексів; (б) розробити відповідний метод; (в) експериментально продемонструвати корисність та придатність запропонованого методу; (г) сформувати та оцінити перелік рекомендованих контрзаходів. Серед використаних методів – Intrusion Modes and Effects Criticality Analysis (IMECA) та тестування на проникнення. **Результати** дослідження: (а) розроблено поетапний метод проактивного аналізу кібербезпеки безпілотних авіаційних комплексів, що поєднує апріорне оцінювання, контрольоване відтворення вибраних режимів вторгнення та апостеріорне уточнення оцінок ризику; (б) розроблено блок-схему проактивного аналізу кібербезпеки безпілотних авіаційних комплексів, яка формалізує процес виявлення вразливостей та дозволяє мінімізувати невизначеність при оцінці ризиків та наслідків вторгнень; (в) для виконання розвідки, сканування вразливостей і виявлення хибних конфігурацій, а також моделювання режимів вторгнення використано SITL платформу, розгорнуту на робочій станції під керуванням Kali Linux; (г) попередньо виявлені режими вторгнення були експериментально підтверджені, що надало змогу для виявлення 35 додаткових режимів вторгнення, пов'язаних між собою наявністю спільної вразливості в протоколі Wi-Fi, з яких 4 потрапили до зони неприйнятного ризику; (д) побудовано апріорні та апостеріорні таблиці IMECA і матриці критичності; (е) сформовано та оцінено перелік рекомендованих контрзаходів. **Висновки**: (а) запропонований метод забезпечує систематичне виявлення режимів вторгнення та емпіричне уточнення оцінок ймовірності, тяжкості наслідків і ризику; (б) наукова новизна полягає у інтеграції методу IMECA з апріорним прогнозуванням та апостеріорним уточненням на основі спостережень, отриманих через застосування процедур тестування на проникнення; (в) розроблена блок-схема виявилась корисною для формалізації виявлення вразливостей і мінімізації невизначеності під час оцінювання ризику; (г) корисність і придатність запропонованого методу було продемонстровано на SITL платформі; (д) аналіз контрзаходів показав, що їх комплексне впровадження усуває всі неприйнятні ризики, знижуючи більшість режимів вторгнення до контрольованої зони ризику, а три режими зберігають залишковий ризик, повне усунення якого потребує архітектурного рішення щодо заміни Wi-Fi як транспортного каналу.

Ключові слова: безпілотний авіаційний комплекс; кібербезпека; IMECA; тестування на проникнення, вразливості, режими вторгнення.

Абакумов Артем Ігорович – асп. каф. кібербезпеки та інтелектуальних інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – член-кореспондент НАН України, д-р техн. наук, проф., зав. каф. кібербезпеки та інтелектуальних інформаційних технологій, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Попов Пітер – д-р філос., доц., заступник декана (з міжнародної діяльності), Школа науки та технологій, кафедра комп'ютерних наук, Університет Сіті Сент-Джорджес, Лондон, Велика Британія.

Artem Abakumov – PhD Student, the Department of Cybersecurity and Intelligent Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: a.i.abakumov@csn.khai.edu, ORCID: 0000-0002-7742-6515.

Vyacheslav Kharchenko – Corresponding Member of the National Academy of Sciences of Ukraine, DrS, Professor, Head of the Department of Cybersecurity and Intelligent Information Technologies, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: v.kharchenko@csn.khai.edu, ORCID: 0000-0001-5352-077X, Scopus Author ID: 22034616000.

Peter Popov – PhD, Associate Professor, Associate Dean (International), School of Science & Technology, Department of Computer Science, City St George's University of London, London, United Kingdom,
e-mail: P.T.Popov@citystgeorges.ac.uk, ORCID: 0000-0002-3434-5272.