Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.078931

ARTICLE

Threat Analysis and Assessment Based on a Collaboration Interface for Manned-Unmanned Teaming Systems

Gaeul Kim[1] **and Dohoon Kim**[2,*]

[1]Department of Software Safety and Security, Kyonggi University, Suwon-si, Republic of Korea
[2]Department of Computer Science, Kyonggi University, Suwon-si, Republic of Korea

*Corresponding Author: Dohoon Kim. Email: karmy01@kyonggi.ac.kr

Received: 10 January 2026; Accepted: 25 March 2026; Published: 08 May 2026

ABSTRACT: Manned-Unmanned Teaming (MUM-T) is an operational system where manned and unmanned systems perform missions through a collaboration interface, expanding beyond defense into civilian domains. The core of MUM-T lies in the organic interaction between manned and unmanned systems. The Collaboration Interface enabling this interaction becomes a primary target for cyber attacks due to its reliance on wireless networks. Compromising the reliability of the collaboration interface goes beyond simple communication failures; it directly leads to mission failure and aircraft safety issues. Therefore, systematic threat analysis and assessment tailored to this specific domain are essential. This study performs threat modeling based on the MITRE ATT&CK framework for the MUM-T collaboration interface and proposes a behavior-based risk assessment methodology combined with multi-criteria decision making (MCDM) techniques. First, attack techniques reflecting the characteristics of the collaboration interface are derived to structure threat scenarios. The relative importance of each TTP of the scenario is quantified to calculate the overall risk. When applied to GPS and battery spoofing scenarios, the proposed methodology confirmed that by structurally reflecting the likelihood of occurrence and propagation paths of TTP units, it precisely derives the complex threat characteristics of MUM-T environments. By defining collaboration interfaces as the analysis target and presenting a TTP-based threat analysis and quantitative risk assessment methodology, this study provides practical grounds for determining threat-specific response priorities in MUM-T environments.

KEYWORDS: Manned-Unmanned Teaming (MUM-T); collaboration interface; threat modeling; TTP-based risk assessment; Multi-Criteria Decision Making (MCDM)

1 Introduction

Manned–Unmanned Teaming (MUM-T) refers to an operational concept in which unmanned systems equipped with autonomous capabilities form a team under the control of a manned system to execute missions [1]. The MUM-T concept originally evolved within the military domain to enhance the survivability of manned aircraft and to maximize operational efficiency [2]. Recently, however, its application has expanded into civilian sectors, including missions such as missing person searches [3,4], large-scale wildfire monitoring [5,6], as well as Urban Air Mobility (UAM) and Advanced Air Mobility (AAM) systems [7]. This expansion demonstrates that MUM-T extends beyond purely military purposes and permeates daily life and various industrial domains.

However, as the operational scope of MUM-T expands, the number of security threats targeting MUM-T systems also increases. In particular, the interfaces that enable collaboration between manned and

unmanned systems inherently rely on wireless networks, which increases their exposure to various cyber attacks [8]. Compromise of the reliability of these collaboration interfaces threatens not only communication integrity and mission success but also the safety of both manned and unmanned aircraft [9,10]. Therefore, systematic analysis and evaluation of the security of collaboration interfaces in a MUM-T environment constitutes a critical task. Existing research on MUM-T security has primarily focused on system architecture design [11] or on strengthening authentication and cryptographic mechanisms [8,12]. Several studies have conducted risk analyses for UAVs or individual unmanned systems. However, research that systematically examines threats related to the collaboration interface remains limited. Such studies rarely treat the manned–unmanned collaboration structure as a single operational system. In particular, approaches that structure identified threats into behavioral units and quantitatively derive their relative importance remain insufficiently explored in the MUM-T environments.

This study proposes a process for threat analysis and quantitative prioritization, focusing on the collaboration interface, which represents the most vulnerable component in the MUM-T environments. The point of interaction between human-operated and unmanned systems is defined as the Collaboration Interface, and a methodology is presented to identify and evaluate security threats centered on this interface. To operationalize this approach, the collaboration interface is first characterized based on the MUM-T architecture. Subsequently, potential security threats within this interface are identified. Tactics, Techniques, and Procedures (TTPs) are mapped using the MITRE ATT&CK framework [13] to model concrete attack scenarios. The risk levels of the derived scenarios are then quantitatively assessed through Multi-Criteria Decision Making (MCDM) techniques [14,15].

This study identified the collaboration interface as the primary target of security threat analysis in the MUM-T environment, clearly defining the key points at which attacks occur and impacts propagate. Threats were structured into TTP units based on the MITRE ATT&CK framework and integrated with MCDM to quantify the relative importance of each TTP. This approach decomposes collaboration interface threats at the behavioral level, identifies corresponding risk mitigation measures, and links them to a quantitative evaluation framework. As a result, it establishes a risk assessment structure that simultaneously reflects attack execution stages and impact propagation. This framework provides a practical foundation for determining response priorities and allocating limited security resources.

The remainder of this paper is organized as follows. Section 2 reviews security research trends based on MUM-T and related studies on threats arising from collaboration interfaces. Section 3 defines collaboration interfaces and presents a systematic process for threat modeling and risk assessment. Section 4 presents the results of applying the proposed methodology to the derived threat scenarios and, analyzes the risk level and operational impact for each scenario. Finally, Section 5 outlines the study's limitations of the study and future research directions, and Section 6 presents the conclusions.

2 Related Work

2.1 Security Research Trends Based on MUM-T

MUM-T is an operational system in which manned and unmanned aircraft form a single team to perform missions. It was developed primarily in the military domain and has recently expanded into the civilian sector. MUM-T requires a framework that extends beyond simple system interconnections, necessitating the systematic management of complex interactions that arise during collaboration between manned and unmanned systems. Woudenberg et al. [11] approached the MUM-T architecture by dividing it into three layers: entity, integrated system, and system security. Their study emphasized the expansion of the cyber attack surface resulting from the proliferation of autonomous technologies. Yang et al. [8]

proposed an authentication technique that combines lightweight cryptographic methods with a blockchain-based distributed architecture to address the single point of failure (SPOF) problem. Yasar and Bahtiyar [12] proposed a hybrid framework that combines a Proof-of-Authority (PoA)-based blockchain with XOR-based lightweight authentication to ensure both data integrity and low-latency communication. While these studies focus on the architectural design of the MUM-T systems or on strengthening communication channel security, they remain limited in providing systematic and specific threat analyses.

This study defines the collaboration interface of MUM-T as the primary unit of analysis and systematically identifies associated threats. Based on this foundation, it constructs an attack chain aligned with the MITRE ATT&CK framework and proposes an evaluation methodology that quantitatively assesses risk levels through the application of MCDM techniques.

2.2 Security Threats to MUM-T Collaboration Interfaces

The MUM-T system aims to enhance the survivability of manned aircraft and extend their mission range by relying on the autonomy of unmanned aerial vehicles (UAVs). The inherent security vulnerabilities of UAVs have become entry points that threaten the reliability of the entire manned-unmanned collaborative network.

For example, GPS spoofing attacks manipulate the location data of UAVs to disrupt the navigation system and, cause collisions or crashes. This is a typical case in which the data integrity is compromised. Sathaye et al. [16] demonstrated through experimental studies on actual UAVs that GPS spoofing extends beyond simple path deviations, allowing attackers to take control of the UAV. Li and Song [17] demonstrated a spoofing attack by intercepting MAVLink packets in an ArduPilot-based simulation environment. This attack introduces false path information to the ground control station (GCS), impairing situational awareness and potentially leading to incorrect control commands. Battery spoofing attacks manipulate telemetry data, causing operators to make erroneous decisions such as premature returns or emergency landings, regardless of the actual battery level. This is a prime example of availability being compromised through integrity violations. Desnitsky and Kotenko [18] presented attack scenarios involving telemetry data tampering over communication channels and highlighted that such attacks risk distorting the entire judgment of the operator beyond simple data falsification or alteration. Eavesdropping attacks on wireless communication channels compromise confidentiality and, leak mission information, whereas Denial-of-Service (DoS) attacks directly undermine communication availability, making mission execution impossible [19].

Existing studies have focused solely on the technical mechanisms of individual threats without addressing, specific methodologies for how these threats combine to evolve into systematic attacks or how to assess the relative risk levels of each threat.

2.3 Existing Risk Assessment Methodologies

In the field of risk assessment, various standards-based methodologies are employed, among which ISO/SAE 21434-based TARA (Threat Analysis and Risk Assessment) [20] and NIST SP 800-30 Rev.1 [21] represent widely adopted approaches. TARA defines threat scenarios as single units of analysis. It presents a procedure for calculating risk levels by integrating attacker capability and system impact factors. Likelihood is evaluated based on attacker capability attributes such as Expertise, Knowledge, Opportunity, and Equipment. Impact is assessed from the perspectives of Safety, Financial, Operational, and Privacy dimensions. TARA also provides procedures for analyzing attack paths at the individual asset or component level. However, its framework addresses the quantitative integration of risk propagation arising from interdependencies between systems only to a limited extent. It does not sufficiently capture cascading effects across interconnected systems. NIST SP 800-30 Rev.1 provides guidelines for conducting risk assessments

for information systems and organizations. It presents structured steps and a systematic model for risk assessment as a core component of the overall risk management process. The OWASP Risk Rating Methodology [22] reflects a similar concept. It evaluates Likelihood based on Threat Agent and Vulnerability factors and derives risk levels by integrating Technical Impact and Service Impact. Although these methodologies provide macro-level assessment frameworks that consider risk propagation at the organizational level, they do not incorporate a structured mechanism that reflects the step-by-step progression through which a threat action connects to a specific technical attack path.

To overcome these limitations, this study decomposes threat scenarios into TTP units based on the threat analysis framework of TARA and evaluates risk at the behavioral level. It derives the final risk level by assigning weights to reflect the relative importance of each TTP. This approach enables an assessment that captures not only the technical contribution of each attack stage but also the manner in which risk propagates through the collaboration interface.

3 Threat Analysis Based on Collaboration Interfaces for MUM-T

This section proposes a methodology for systematically analyzing and evaluating threats centered on the collaboration interface within the MUM-T environment. Section 3.1 defines the collaboration interface based on the MUM-T architecture, and Section 3.2 presents a threat modeling and risk assessment process utilizing the MITRE ATT&CK framework and MCDM techniques.

3.1 Defining Collaboration Interface of MUM-T Architecture

MUM-T is a complex system in which manned and unmanned vehicles form a single team to organically perform missions. Fig. 1 shows the overall architecture of MUM-T considered in this study. The primary systems of the MUM-T platform consist of a Manned Aircraft System, Unmanned Aircraft System, and Mission Ground System, each connected via Command and Control (C2) links. In this study, the points of contact within the MUM-T architecture where practical interactions occur—such as data exchange between heterogeneous assets and the transmission of control commands—are defined as collaboration interfaces. These interface functions as a boundary that goes beyond a mere communication channel, representing externally exposed interaction points through which coordination between system components is achieved. These interfaces serve as the primary targets for threat analysis, including attack surface modeling and adversarial TTP mapping, within the proposed methodology. Collaboration interfaces are broadly classified into two types based on their target and communication purpose [23].

- Manned-Unmanned Communication Module (air-to-air): A direct communication channel between manned and unmanned aircraft, responsible for transmitting control commands from the manned aircraft and sensor data from the unmanned aircraft. It is the core of real-time collaborative operations and the most critical attack surface.
- Manned/Unmanned-Ground Communication Module (air-to-ground): A communication link between ground control stations and manned/unmanned aircraft, transmitting and receiving telemetry data such as mission planning, status monitoring, and position information.

The compromised reliability of these collaboration interfaces extend beyond communication loss or mission failure to the safety of manned and unmanned aircraft.

The red boxed areas in Fig. 1 represent the collaboration interfaces defined in this study—the communication modules in which data exchange between manned and unmanned systems actually occurs. These interfaces transmit control commands, sensor data, and telemetry information via wireless networks and serve as primary entry points for attackers. If the reliability of collaboration interfaces is compromised, the

consequences extend beyond mere communication disruptions and affect the entire collaborative structure. The modules highlighted in green boxes are areas that rely on data received from collaboration interfaces to make decisions. These points are where threats have a significant impact if the interfaces are compromised. If manipulated data enter through collaboration interfaces, they are processed as legitimate information, potentially leading to problems such as navigation system malfunctions, distorted situational awareness, and incorrect mission execution. For example, if a GPS spoofing attack occurs at an air-to-air interface, the manned aircraft cannot determine the actual position of the unmanned aircraft, thereby paralyzing situational awareness. If telemetry data are manipulated at the air-to-ground interface, operators make erroneous decisions, such as ordering an emergency landing, regardless of the actual status of the UAV. This study identifies and analyzes threats by, focusing on the collaboration interface within the overall system, which is vulnerable to security breaches and has significant ripple effects.

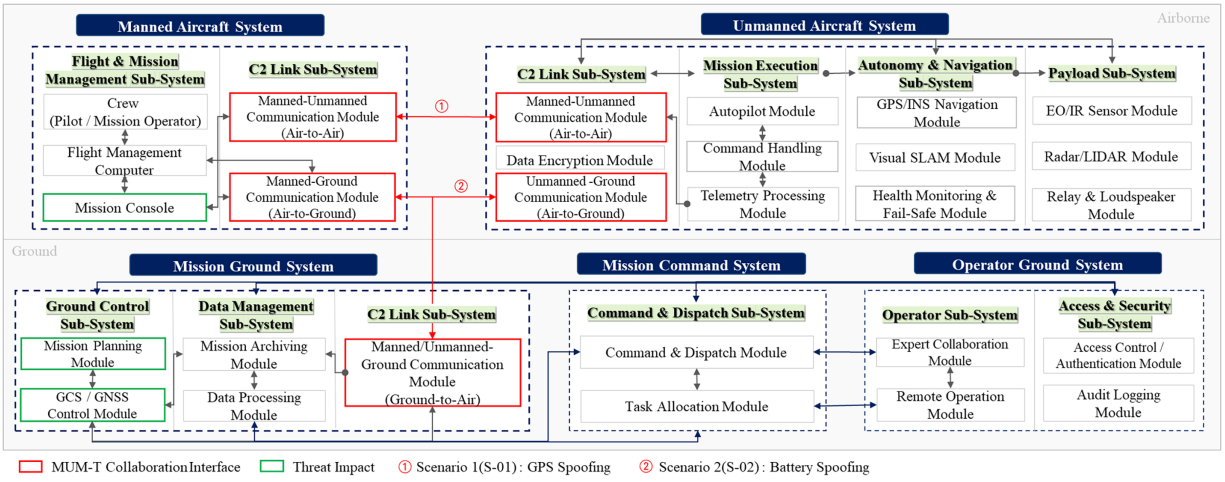


Figure 1: MUM-T architecture.

3.2 Proposed Threat Analysis and Risk Assessment

This section presents a systematic models of the potential threats at collaboration interfaces and proposes a methodology for quantitatively assessing risks. Fig. 2 illustrates the overall process of the proposed methodology.

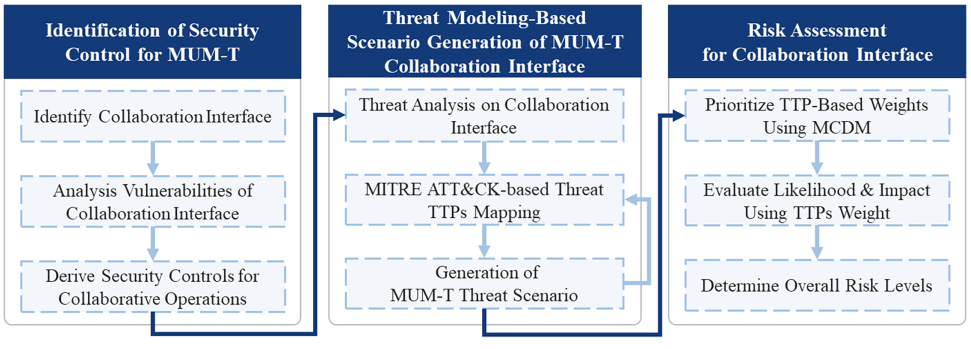


Figure 2: Proposed threat analysis and risk assessment process for MUM-T.

The proposed methodology comprises three main steps. First, security control requirements for the collaboration interface are identified. Next, threat modeling-based scenarios are generated using the MITRE ATT&CK framework. Finally, the risk levels of the selected TTPs are quantitatively assessed.

3.2.1 Identification of Security Control for MUM-T

In the first stage, this study analyzes vulnerabilities inherent to the collaboration interface and derives the affected security properties based on the CIA triad: Confidentiality, Integrity, and Availability. The Collaboration Interface relies on wireless communication channels to enable real-time data exchange between manned and unmanned assets [24]. Such reliance introduces inherent security vulnerabilities. Owing to the open nature of wireless channels, attackers intercept or interfere with communications within radio signal range without physical access [8]. Collaborative environments that require real-time control and low-latency communication introduce a trade-off between protocol complexity and security functionality. This trade-off constrains the implementation of security mechanisms, including encryption and authentication. These vulnerabilities collectively establish an attack surface in environments where continuous data exchange occurs during collaborative missions. The resulting compromised security properties are classified as follows [25,26]

- Confidentiality: Eavesdropping on communication data through wireless channels leads to the exposure of mission information, route planning, and sensor data.
- Integrity: Without encryption and authentication, GPS coordinates or telemetry data are subject to tampering during transit, allowing false information to be injected.
- Availability: Mission execution is interrupted owing to communication disruption from DoS attacks or induced operator misjudgment from manipulated data.

This step identifies the list of threats to the collaboration interface, security attributes compromised by each threat, and affected system areas.

3.2.2 Threat Modeling-Based Scenario Generation

In the second phase, specific attack scenarios are generated for previously identified threats using the MITRE ATT&CK framework. This study performed threat modeling using the MITRE ATT&CK framework to define the specific attack techniques and procedures associated with the identified threats. MITRE ATT&CK is a knowledge base that classifies attackers TTPs based on real cyberattack cases. It is used as a standard for threat analysis across various domains.

This study identified the objectives and execution methods of attackers to formalize attacks targeting the MUM-T collaboration interface, thereby deriving threat scenarios. First, considering the MUM-T operational environment, four criteria were applied to identify valid attack tactics [27,28]. The feasibility measure assesses whether a tactic/technique is theoretically feasible within the threat scenario and target elements. The necessity measure assesses whether the technique is indispensable for the construction of an attack chain during execution. The implementability measure verifies whether the technique is practical in a real environment, considering the wireless communication environment and the MUM-T system characteristics. The impact measure considers the ripple effect of the attack on mission execution and collaborative operations. Based on these criteria, we selected tactics applicable to the MUM-T environment. We performed a pairwise comparison analysis to evaluate the relative importance of each technique. Based on this analysis, core techniques were identified from the selected candidate techniques for constructing attack scenarios. Pairwise comparison analysis quantifies the relative importance of multiple alternatives by comparing them in pairs. It is one of the core techniques in MCDM. The TTPs identified in this study perform

distinct functions at different stages of the attack chain. The scope and persistence of their impact on mission execution also vary. Accordingly, the importance of each TTP is more appropriately derived from its relative contribution under a common comparison criterion, rather than being independently assigned a single numerical value. The objective of this study lies not in estimating the probabilistic risk of individual TTPs, but in identifying the techniques that deserve primary consideration within attack scenarios. To achieve this objective, the MCDM methodology is applied to derive relative importance among the identified techniques. To conduct the pairwise comparison analysis under consistent evaluation criteria, comparison values were determined based on relevant literature [29]. This approach derives comparison values according to the structural role each TTP performs within an attack scenario. The literature establishes common comparison criteria, including the functional role of each TTP within the attack, the uniqueness of that role, and the scope and persistence of its impact on system behavior and operational decision-making. The criteria for reference selection and pairwise comparison are detailed in Appendix A.

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & 1 & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & 1 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & 1 \end{pmatrix}, \qquad a_{ij} = \frac{1}{a_{ji}}, \qquad a_{ii} = 1 \tag{1}$$

$$A\mathbf{w} = \lambda_{\max}\mathbf{w} \tag{2}$$

The pairwise comparison matrix $A = [a_{ij}]$ is an $n \times n$ matrix, where each element a_{ij} represents the relative importance of technique i over technique j. The principal eigenvector of the comparison matrix A is computed to obtain the weight vector $\mathbf{w} = [w_1, w_2, \ldots, w_n]$. The eigenvectors were computed using the geometric mean method, which serves as a widely adopted practical approximation for the principal eigenvector. The resulting vector was normalized to obtain the weight vector, and the maximum eigenvalue $\lambda_{\max}$ was subsequently estimated based on this normalized vector. The Consistency Index (CI) and Consistency Ratio (CR) are calculated as follows

$$CI = \frac{\lambda_{\max} - n}{n - 1}, \qquad CR = \frac{CI}{RI} \tag{3}$$

where n denotes the number of techniques being compared, and RI represents the random index. In general, if $CR < 0.1$, the consistency of the comparison matrix is assured. Once the consistency of the matrix has been validated, TTPs are prioritized based on their relative importance. The calculated weights are sorted in descending order, and the top TTPs with cumulative weights of 90% or higher are selected as the final attack techniques. This approach maintains a 90% confidence level for the overall threat while selecting only the core attack techniques, thereby enhancing the effectiveness of the scenario [27]. The derived TTPs represent specific procedures performed by an attacker to compromise the collaboration interface. Based on this, an attack chain is constructed and a risk assessment is conducted.

3.2.3 Risk Assessment for Collaboration Interface

Finally, a quantitative risk assessment is performed on the final set of TTPs for each scenario. The purpose of this step is to calculate the weights reflecting the relative importance of TTPs within each scenario, assess the likelihood and impact of each TTP, and integrate these factors using a weighted-sum method to calculate the scenario-level risk. Quantitative risk assessment comprises evaluation factors defined at the TTP level and scenario-level outcome metrics derived by integrating these factors as follows:

- **Likelihood** (L_i): TTP i is a score evaluating the likelihood of occurrence within an attack scenario, serving as an input for calculating the overall probability of the occurrence of the scenario.
- **Impact** (I_i): The score evaluating the impact on the MUM-T collaborative mission performance when TTP i is successfully executed, serving as an input for calculating the overall scenario impact.
- **Weight** (w_i): The weights representing the relative importance of the TTPs ultimately selected within the scenario, calculated through pairwise comparison analysis, are normalized such that the sum of all TTP weights equals 1.

By combining these elements, intermediate outputs are defined to quantitatively express the extent to which each TTP contributes to the overall scenario risk assessment. In this study, these are defined as the weighted likelihood contribution ($L_i \times w_i$) and weighted impact contribution ($I_i \times w_i$).

First, a pairwise comparison-based analysis is performed on the final set of TTPs selected for each scenario to calculate the relative importance of each TTP. This process comprehensively considers the role and position each TTP plays within the attack scenario, as well as its contribution to the attack flow. This yields a weighted vector $\mathbf{w} = [w_1, w_2, \ldots, w_n]$ that quantifies the relative importance among TTPs, with all weights normalized to a sum of 1. Next, the likelihood (L_i) and impact (I_i) of each TTP are evaluated independently for the set of TTPs. At this stage, scores are assigned based on the inherent characteristics of each TTP and its functional significance within the scenario, regardless of the magnitude of its weight. This enables the quantification of the occurrence probability and impact level per TTP. Based on the calculated L_i, I_i, and w_i values, the weighted likelihood contribution and weighted impact contributions are computed for each TTP. These values are then summed to derive the overall likelihood and impact of the threat scenario. The weighted likelihood (L_t) and weighted impact (I_t) are defined as follows:

$$L_t = \sum_{i=1}^{n} (L_i \times w_i), \qquad I_t = \sum_{i=1}^{n} (I_i \times w_i). \tag{4}$$

Based on these formulations, the weighted-sum method reflects the relative importance of individual TTP scores in the aggregation process. TTPs that play a pivotal role in the attack chain have a greater impact on the overall risk level. The derived weights (w_i) represent the relative contributions of each TTP within the attack chain and indicate their significance to the overall success of the scenario. As a result, TTPs with higher weights exert a greater influence on the final risk calculation, making it easier to identify which attacks play a critical role in the overall risk. The calculated weighted likelihood (L_t) and weighted impact (I_t) are mapped onto a 5 × 5 risk matrix [21] to determine the final risk level for each scenario. The position on the risk matrix helps prioritize limited security resources and serves as a criterion for classifying risk levels. This study adopts the risk matrix concept presented in NIST SP 800-30 Rev.1 for risk assessment.

4 Experimental Results and Analysis

This section presents the results of applying the threat analysis and risk assessment process proposed in Section 3 to potential threats arising within the MUM-T collaboration interface. The experimental environment was constructed using the engine of DVD (Damn Vulnerable Drone) [30], a drone simulator specifically designed to incorporate security vulnerabilities. DVD utilizes ArduPilot and the MAVLink protocol to replicate the communication architecture of real-world drone systems, including their known vulnerabilities, thereby providing a virtual environment for testing and verifying attack scenarios. Within this environment, GPS spoofing and battery spoofing scenarios relevant to the collaboration interface were implemented. The attacks were replicated by intercepting and manipulating MAVLink protocol messages. Detailed information about the operating system, container configuration, communication architecture, and monitoring framework of the experimental setup is provided in Appendix B.

4.1 Security Control Identification

This section analyzes vulnerabilities arising within collaboration interfaces and identifies compromised security attributes based on the CIA triad: Confidentiality, Integrity, and Availability. This study emphasizes that manipulation of telemetry information exchanged through the collaboration interface exerts a structural influence on the overall mission execution and decision-making process. In manned–unmanned collaborative systems, location data and energy status information serve as critical inputs for path maintenance, formation control, and mission persistence decisions. Tampering with such information destabilizes the collaborative system beyond isolated data errors. These characteristics define a primary threat category for analyzing information manipulation attacks targeting the collaboration interface. S-01 (GPS Spoofing) and S-02 (Battery Spoofing), shown in Fig. 1, were selected as the primary subjects of analysis. These scenarios represent cases that compromise Integrity and Availability, respectively, through direct manipulation of telemetry data exchanged within the collaboration interface.

- S-01 (GPS Spoofing): GPS spoofing compromises the integrity of the position and navigation data of an unmanned aircraft. When counterfeit GPS signals are injected, flight path deviations and safety system malfunctions occur, rendering command and control of the aircraft impossible.
- S-02 (Battery Spoofing): Battery spoofing compromises system availability by manipulating telemetry data. When battery status information is falsified, pilots make misjudgments, causing UAVs to disengage from the battlefield, which results in the collapse of collaborative mission sustainability.

The results of the TTP selection process, which is conducted based on the MITRE ATT&CK framework to generate specific attack scenarios for the two identified threats are detailed in the following section.

4.2 Generated Threat Scenarios

This section constructs concrete attack scenarios for each threat identified in Section 4.1 by applying the MITRE ATT&CK framework described in Section 3.2.2. Using S-01 as a representative example, the procedure is presented step-by-step, beginning with the derivation of candidate TTPs and followed by the selection of core TTPs through filtering and weighting processes. The results obtained from applying the same procedure to S-02 are also summarized. Mapping the MITRE ATT&CK TTPs to S-01 produced numerous candidate Techniques across 10 Tactics, ranging from Reconnaissance to Impact. To refine the selection, TTPs were filtered according to Feasibility, Necessity, Implementability, and Impact in order to construct meaningful and realistic attack scenarios. Through this process, ten TTP candidates satisfying all four criteria were identified: T1592, T1133, T1059, T1562, T1036, T1040, T1046, T1090, T1565, and T1491.

A pairwise comparison analysis was conducted to select core TTPs from the identified candidate pool. This process quantified the contribution of each TTP to GPS spoofing attacks by pairing ten TTPs in pairs to compare their relative importance. Pairwise comparisons was conducted based on relevant academic literature and attack case studies, and the results are listed in Table 1.

As shown in Table 1, a pairwise comparison matrix was constructed to derive the weight vector by solving the corresponding eigenvalue problem. The maximum eigenvalue was found to be $\lambda_{max} = 10.793$, resulting in $CI = 0.088$ and $CR = 0.059$. Since $CR < 0.1$, the consistency of the comparisons is considered acceptable. After sorting the weights in descending order, T1565 (Data Manipulation) exhibited the highest weight, followed by T1036 (Masquerading) and T1090 (Proxy). These results indicate that the success of the attack primarily depends on manipulating GPS data disguised as legitimate information, along with establishing a communication relay structure to sustain transmission. Applying a cumulative weight threshold of 90% resulted in the selection of seven TTPs, as shown in Table 2. The same procedure was applied to S-02. The resulting consistency ratio was $CR = 0.011$, which satisfies the acceptable threshold. Applying

the 90% cumulative weight criterion resulted in the selection of five core TTPs, as shown in Table 2. The detailed procedure for constructing the pairwise comparison matrix and calculating the weights is provided in Appendix A.

Table 1: Pairwise comparison matrix of selected TTPs for scenario S-01.

	T1592	**T1133**	**T1059**	**· · ·**	**T1491**
T1592	1	1/5	1/7	· · ·	1/3
T1133	5	1	1/3	· · ·	3
T1059	7	3	1	· · ·	5
⋮	⋮	⋮	⋮	⋱	⋮
T1491	3	1/3	1/5	· · ·	1

Table 2: Threat scenarios and selected TTPs.

Threat Scenario	**CIA Impact**	**Affected System**	**Interface Type**	**Selected TTPs**
S-01 (GPS Spoofing)	Integrity	Mission console	Air-to-Air	T1133, T1059, T1036, T1040, T1090, T1565, T1491
S-02 (Battery Spoofing)	Availability	Mission planning module, GCS/GNSS control module	Air-to-Ground	T1190, T1557, T1059, T1565, T1489

The attack flow in the final threat scenario is shown in Fig. 3. S-01 represents an attack in which an attacker injects false coordinate data through an MAVLink proxy, as shown in Fig. 3. The UAV GPS/INS navigation module typically generates actual GPS coordinates and transmits them to the manned aircraft. However, the attacker can intercept these normal data during Manned-Unmanned communication, replace it with manipulated coordinates, and delivers it to the manned aircraft. The falsified GPS data is displayed on the mission console of the manned aircraft. The pilot mistakenly believes that the drone deviated from its normal route and fall into a 'blind' state, unable to determine the position of the drone, thereby, rendering mission execution impossible. The UAV operates normally and flies along the actual route; however, the manned system operator has no choice but to trust the manipulated information, thereby paralyzing situational awareness.

S-02 represents an attack in which the attacker intercepts and manipulates data mid-transmission during Manned/Unmanned-Ground communication. The attacker intercepts the actual battery status data transmitted from the Telemetry Processing Module of the UAV, reduces the remaining battery level to 0%, and delivers it to the Mission Ground System and Manned Aircraft System. This manipulated information triggers a "LOW BATTERY ALERT" warning in the GCS/GNSS Control Module, and the Mission Planning Module determines that the battery level has decreased below the critical threshold. The pilot, trusting the system warning, issues a return command to the UAV. The UAV departs from the battlefield regardless of the actual battery level. The attacker compromises the availability of an unmanned asset by inducing an erroneous decision by the operator without directly seizing control.

In both scenarios, the Unmanned Aircraft System operates normally and generates real data; however, the manipulated data are transmitted during the data transfer process via a collaboration interface owing to attacker intervention. This demonstrates that the collaboration interface represents the most vulnerable attack surface in the MUM-T environment.

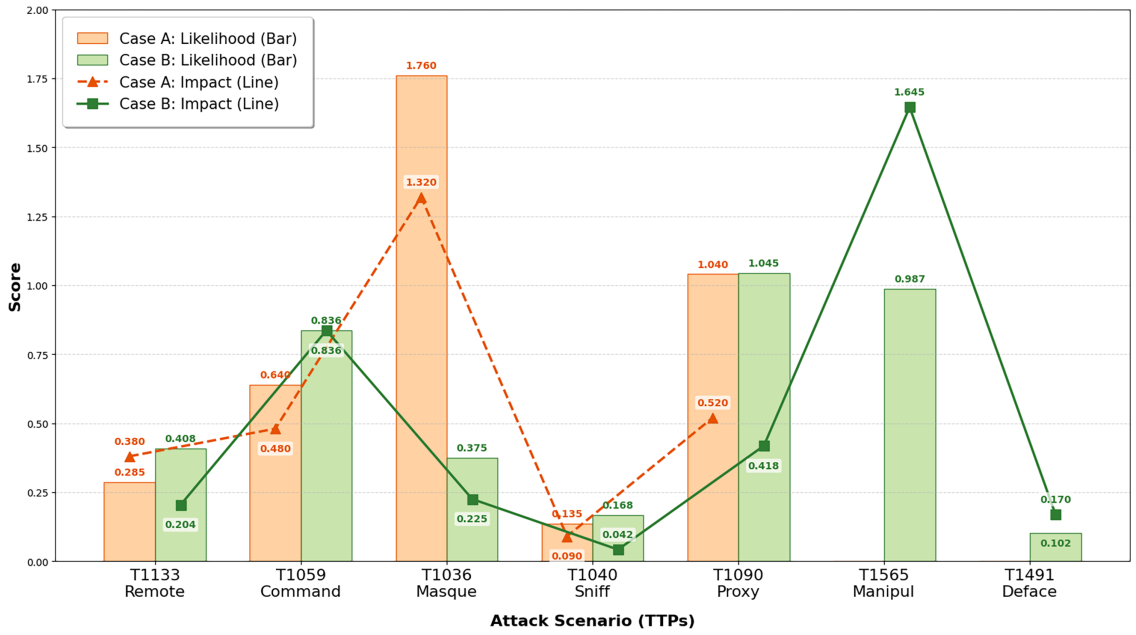


Figure 3: Comparison of weighted TTPs contributions for S-01.

4.3 Quantitative Risk Assessment

In this section, the final risk level is calculated quantitatively based on the TTPs that constitute the generated threat scenarios, as described in Section 3.2.3. When assessing threats to the MUM-T collaboration interface, the evaluation results vary depending on how the scope of the TTP analysis target is defined. The set of TTPs differs depending on whether the assessment is limited to attack actions directly occurring at the collaboration interface or if it also includes the system areas affected by the propagation of the impact of the attack. Risk assessments were performed to analyze the effect of these scope differences on the final risk level by defining two categories of TTP sets.

- Case A: Targets the set of TTPs associated with attack actions directly executable at the collaboration interface within the MUM-T architecture, treating the collaboration interface itself as the primary attack surface.
- Case B: In addition to the TTPs of Case A, it includes TTPs related to the affected system domain where attack results propagated through the collaboration interface are transmitted. This encompasses not only the attack actions themselves but also TTPs related to the impact of those results on the entire MUM-T collaborative operation, including navigation systems, mission management, and status monitoring. It is a superset of Case A.

Similarly, a pairwise comparison analysis was performed for each case to calculate the relative importance of the TTPs. The pairwise comparison matrix and weight calculation process for S-01 are listed in Tables 3 and 4, respectively, and the same procedure was applied for S-02.

To verify the reliability of the pairwise comparison results for each case presented in Tables 3 and 4, the CR was calculated. For S-01, $CR = 0.018$ was obtained for Case A and $CR = 0.039$ for Case B. For S-02, $CR = 0.002$ and $CR = 0.0164$ were obtained for Case A and Case B, respectively. In all cases, the values satisfy the condition $CR < 0.1$ indicating acceptable consistency. Based on the calculated weights, the likelihood (I_i) and impact (L_i) of each TTP were evaluated. The Weighted Likelihood Contribution and Weighted Impact

Contribution were then derived. A comparison of the weighted contributions for each TTP between Case A and Case B is presented in Figs. 4 and 5.

Table 3: TTP weight calculation for S-01 (Case A).

	T1133	T1059	T1036	T1040	T1090	Weight
T1133	1.000	0.500	0.200	3.000	0.333	0.042
T1059	2.000	1.000	0.333	4.000	0.500	0.085
T1036	5.000	3.000	1.000	7.000	2.000	0.233
T1040	0.333	0.250	0.143	1.000	0.200	0.176
T1090	3.000	2.000	0.500	5.000	1.000	0.464
Sum						1.000

Table 4: TTP weight calculation for S-01 (Case B).

	T1133	T1059	T1036	T1040	T1090	T1565	T1491	Weight
T1133	1.000	0.500	0.333	3.000	0.333	0.200	3.000	0.076
T1059	2.000	1.000	0.333	3.000	1.000	0.250	4.000	0.116
T1036	3.000	3.000	1.000	5.000	2.000	0.333	5.000	0.215
T1040	0.333	0.333	0.200	1.000	0.250	0.143	2.000	0.042
T1090	3.000	1.000	0.500	4.000	1.000	0.333	4.000	0.141
T1565	5.000	4.000	3.000	7.000	3.000	1.000	6.000	0.376
T1491	0.333	0.250	0.200	0.500	0.167	0.167	1.000	0.034
Sum								1.000

Figs. 4 and 5 illustrate how the contribution of each TTP varies according to the scope of analysis. Case A considers attack activities conducted directly within the collaboration interface. In contrast, Case B extends the scope to include the propagation of attack consequences across the entire collaborative structure. This difference in analytical scope leads to corresponding changes in the weighted contribution of each TTP. Fig. 4, which illustrates Scenario S-01, shows that in Case A, T1036 (Masquerading), representing the technical core of attack execution, exhibits the highest contribution, with a Likelihood of 1.760 and an Impact of 1.320. This result reflects the critical role of masquerading actions in ensuring attack success within the collaboration interface. In this configuration, the evaluation structure emphasizes the likelihood of successful attack execution. In contrast, Case B expands the analytical scope to incorporate impact propagation across the collaborative structure. Under this scope, outcome-oriented TTPs receive greater weight. Notably, T1565 (Data Manipulation) exhibits the highest Impact contribution at 1.645. Forged packets directly influence system-wide decision-making and mission execution, thereby amplifying their overall effect. The focus of risk assessment shifts from the mechanics of attack execution to the systemic consequences that propagate throughout the collaborative structure. In Fig. 5, S-02 exhibits a similar pattern. In Case A, T1557 (MitM) shows the highest Likelihood contribution (3.240), highlighting the technical feasibility of attack execution. In Case B, T1565 (Data Manipulation) records the highest Impact contribution (1.752). These results indicate that even when the same set of TTPs is considered, the risk contribution structure varies according to the analytical scope.

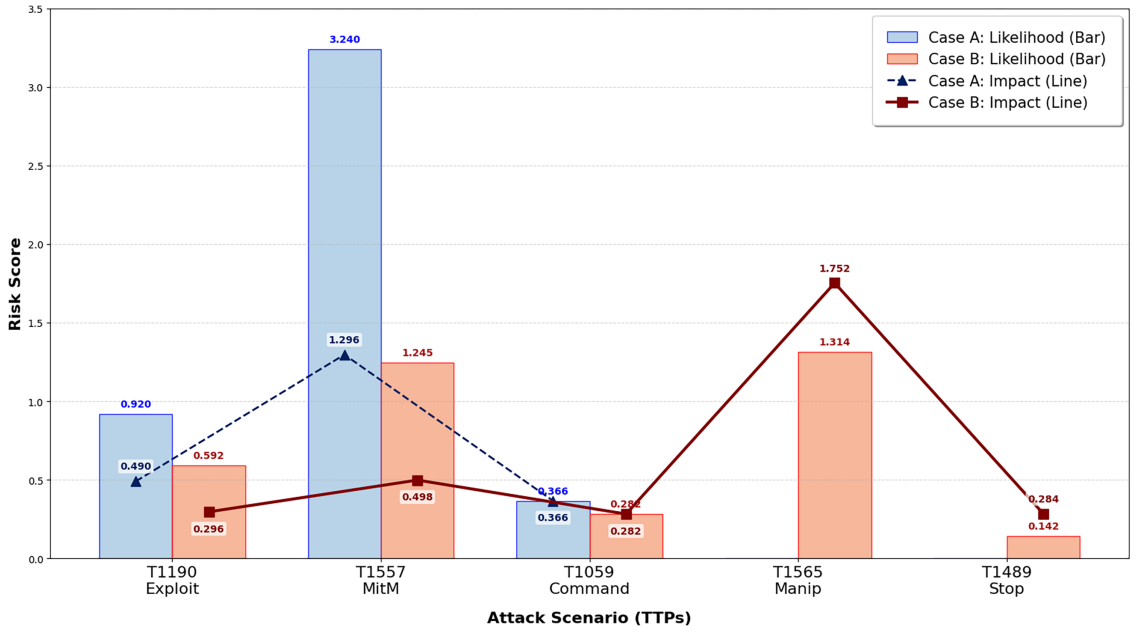
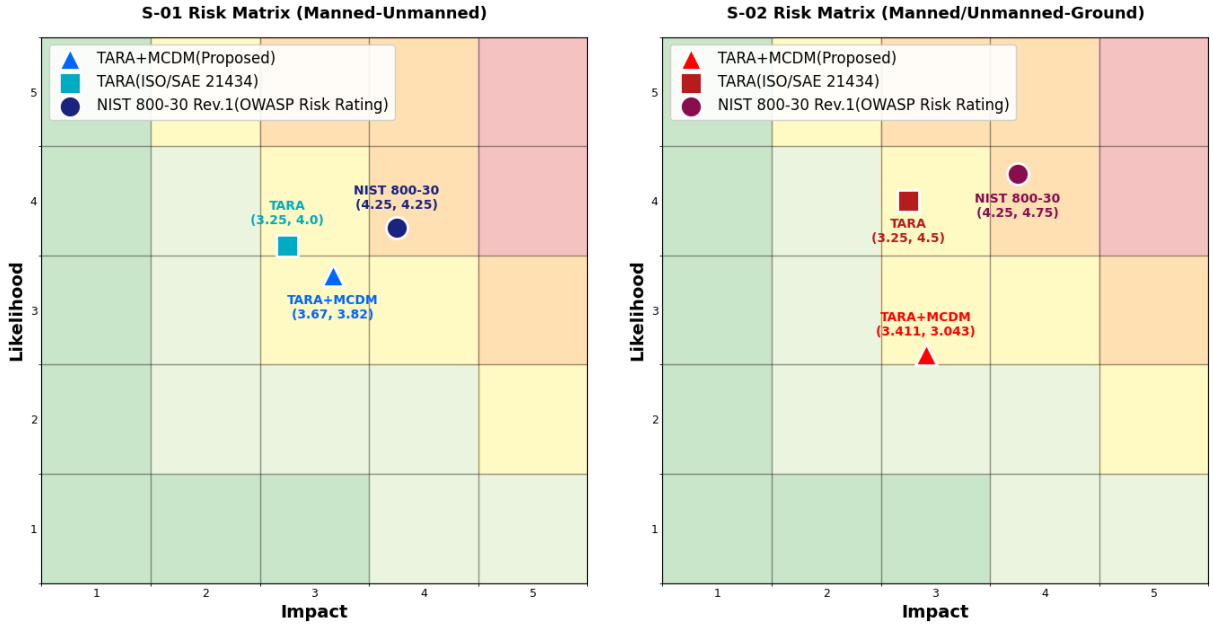


Figure 4: Comparison of weighted TTPs contributions for S-02.



(**a**) (**b**)

Figure 5: Comparison of risk assessment results by methodology: (**a**) S-01 risk matrix (Manned–Unmanned); (**b**) S-02 risk matrix (Manned/Unmanned–Ground).

The Weighted Likelihood (L_t) and Weighted Impact (I_t) for each scenario were calculated by aggregating the TTP-specific contributions. The resulting values were then mapped onto the Risk Matrix, and the outcomes are presented in Table 5.

The risk assessment results presented in Table 5 reveal a consistent difference in risk levels between Case A and Case B for both S-01 and S-02.

Table 5: Comparison of risk level calculations between case A and case B for S-01 and S-02 scenarios.

Scenario	Case	Weighted Likelihood (L_t)	Weighted Impact (I_t)	Risk Level
S-01	Case A	3.600	2.955	LOW
	Case B	3.673	3.817	MEDIUM
S-02	Case A	4.526	2.77	LOW
	Case B	3.575	3.112	MEDIUM

Case A considers only attack actions occurring within the collaboration interface. Under the S-01 criteria, the Weighted Likelihood (L_t) reached 3.600, whereas the Weighted Impact (I_t) remained at 2.955 because the scope of impact was confined to the interface level. Similarly, S-02 produced a high Likelihood value of 4.526, while its Impact was limited to 2.77. Although the probability of attack success was evaluated as high, the broader mission-level consequences were not fully incorporated. As a result, both scenarios were classified as LOW. Case B incorporates the propagation of attack consequences throughout the collaborative structure. Indirect effects, including situational awareness errors, distorted decision-making, and mission execution delays, are reflected in the Impact calculation. Under this scope, the Weighted Impact (I_t) for S-01 increased to 3.817, and that of S-02 rose to 3.112. Although the Likelihood values remain similar to those in Case A, the increased Impact elevates both scenarios to the MEDIUM level.

These findings indicate that assessing risk solely based on the likelihood of an attack leads to an underestimation of mission-level threats. Case A reflects a technology-centered, localized assessment perspective, whereas Case B expands the evaluation to include mission-wide consequences. In collaborative systems such as MUM-T, the critical risk factor lies not only in whether an attack is executed but also in the systemic impact of its consequences. An approach that integrates both technical feasibility and impact propagation offers a more realistic representation of the overall risk structure. Accordingly, threat prioritization and mitigation strategies should be determined based on the extent of impact propagation throughout the mission. Evaluations limited to interface-level effects result in the misclassification of critical threats and lead to insufficient defensive measures. Incorporating mission-level impact into the assessment supports a more effective allocation of security resources in real MUM-T operations.

Based on this analysis, the functional impact of the risks assessed from the Case B perspective on the MUM-T collaborative structure is examined. Although S-01 and S-02 involve different attack vectors, both can be interpreted within the MUM-T environment as state-awareness disruption attacks. These attacks distort the state information perceived by the system and thereby influence the execution of collaborative missions. When such an attack succeeds, its impact does not remain confined to the initially targeted asset. Instead, it propagates throughout the collaborative structure via the collaboration interface, progressively affecting the entire system.

- Loss of trust in collaborative input information: A major derived threat of state-awareness disruption attacks is the degradation of the trustworthiness of the state information used during the collaboration process. When location or energy-status information is perceived as inconsistent with the actual state, that information no longer functions as reliable data.
- Distortion of situational awareness and decision-making: When compromised state information is shared through the collaboration interface, both manned and unmanned assets perceive the situation based on information that is inconsistent with the actual environment. This distorts collaborative decision-making during mission execution, including spatial judgment, mission-continuity assessment,

and asset placement decisions, ultimately lowering the situational awareness of operators in the MUM-T environment.

- Instability in collaborative structures and mission failure: As decision-making distortions accumulate, the role allocation and consistent mission flow between assets required in the MUM-T environment become difficult to maintain. This leads to repeated unexpected mission departures by specific assets, disruptions in collaborative pathways, or mission readjustments, ultimately resulting in instability within the collaborative structure and mission failure.

4.4 Comparison with Risk Assessment Method

To validate the effectiveness of the behavior-based risk assessment methodology proposed in this study, a comparative analysis was conducted against ISO/SAE 21434-based TARA (Threat Analysis and Risk Assessment) and the OWASP Risk Rating Methodology. All three methodologies were applied to the same two threat scenarios to compare their evaluation perspectives and resulting risk levels. This comparison clarifies the structural differences between existing risk assessment approaches and the proposed methodology. The Risk Matrix employed in this study was constructed based on the risk calculation model presented in NIST SP 800-30 Rev.1. It adopts the same 5 × 5 matrix structure and evaluation scale as existing standard methodologies, enabling objective comparison of assessment outcomes.

The methodological core of this study lies in shifting the unit of risk assessment analysis from the scenario level to the TTP level. Existing approaches evaluate threat scenarios as single integrated units. In contrast, this study treats individual TTPs as independent analysis units and derives risk by incorporating their relative importance as weights. This structure enables an assessment that accounts for both the technical feasibility of attack execution and the propagation of impact within the collaborative structure. The differences in evaluation criteria, analysis units, and risk calculation methods among the three methodologies are summarized in Table 6. The risk assessment results for the two threat scenarios under each methodology are presented in Fig. 5.

Table 6: Comparison of structural differences between NIST SP 800-30 Rev.1, TARA, and the proposed methodology.

Category	NIST 800-30 Rev.1 (OWASP Risk Rating)	TARA (ISO/SAE 21434)	TARA+MCDM (Proposed)
Methodology Type	Risk scoring approach	Threat modeling-based risk assessment	Threat modeling-based weighted risk assessment
Analysis Unit	Threat event (Scenario)	Threat scenario	**TTPs**
TTP Consideration	△ (Event-level reference to threat techniques)	△ (Referenced in attack path construction)	**O**
Attack Path Analysis	**X** (No structured attack path analysis)	**O** (Technical path & feasibility analysis)	**O**
Risk Propagation	△ (Organizational-level risk aggregation)	**X** (System-level evaluation scope)	**O** (Interface-centric propagation modeling)
Likelihood Evaluation	Threat agent/vulnerability factors	Attacker capability-based factors	Likelihood of TTP
Impact Evaluation	Technical/Business impact	SFOP impact (Safety, Financial, etc.)	Impact of TTP (mission impact)

Fig. 5 presents the results of applying NIST SP 800-30 Rev.1, TARA, and the proposed risk-assessment methodology to each threat scenario on a risk matrix.

Fig. 5a presents the results for S-01. Under the NIST-based evaluation, the risk level is positioned at (4.25, 4.25), placing it in the HIGH region. TARA yields (3.25, 4.0), reflecting a decrease along certain dimensions while maintaining a relatively elevated risk level. In contrast, the proposed method is located at (3.67, 3.82), corresponding to the MEDIUM region and indicating a shift in matrix position compared to existing approaches. A similar pattern appears in Fig. 5b. NIST is evaluated at (4.25, 4.75), and TARA at (3.25, 4.5). The proposed method, however, is positioned at (3.41, 3.04), further demonstrating a change in risk classification. The positional differences observed in Fig. 5 arise from structural distinctions in how each methodology defines and constructs risk.

The NIST SP 800-30 Rev.1-based assessment calculates risk with Threat Events as the central unit of analysis. It evaluates likelihood by combining threat source characteristics, such as Capability and Intent, with vulnerability factors. This structure exhibits characteristics of conceptual coupling and aggregation of individual threat factors. As a result, various attack stages within a scenario tend to converge into a single aggregated risk level. So, scenarios involving complex attack paths are often assessed at relatively high risk levels. However, in collaborative environments where multiple assets are organically interconnected, this approach presents limitations. It becomes difficult to precisely distinguish the varying degrees of impact that individual attack actions exert on mission execution.

The TARA methodology structures attack paths around defined threat scenarios and evaluates their feasibility based on the attacker's capabilities. Because the technical skill level and resource requirements for executing an attack are directly incorporated into this evaluation, the calculated likelihood tends to be lower than that obtained from NIST-based assessments. Risk evaluation is generally confined to the scope of specific systems or assets. Although technical attack path analysis is conducted with precision, the model does not explicitly incorporate the propagation of impact to other assets through collaboration interfaces after an attack succeeds. As a result, impact is primarily assessed based on damage to the targeted asset itself. Elevated risk values may remain when substantial loss of asset functionality or mission degradation is identified.

The proposed methodology decomposes threat scenarios into TTP units. It evaluates the likelihood of occurrence and mission impact for each TTP individually. The final risk level is calculated through weighted aggregation of these contributions. Existing approaches treat the entire attack path as a single analytical element. As a result, risk tends to be aggregated in a conservative manner. In contrast, the proposed method separates technical execution difficulty from mission-level impact. Each factor is independently reflected in the risk calculation structure. As shown in Fig. 5, Likelihood is adjusted based on the technical difficulty of the TTPs that substantively contribute to attack execution, rather than on an abstract scenario-based probability of occurrence. Impact is assessed according to Mission Impact criteria within the MUM-T collaborative system, rather than based on the magnitude of damage to individual assets. The final classification of risk as MEDIUM does not indicate a simple numerical decrease. It represents a reinterpretation of the threat resulting from the concretization of evaluation units and the refinement of impact representation.

The comparative analysis conducted earlier showed that the results of a risk assessment vary depending on the perspective and analysis unit adopted, even for the same threat scenario. These differences are closely related to the assessment method and structural characteristics of the operational environment being evaluated.

In the MUM-T environment, manned and unmanned aircraft continuously exchange information through a collaboration interface to perform missions. Therefore, when an attack occurs, its consequences are

not limited to a single asset, but affect other assets and functional areas along the collaborative flow. Therefore, assessing risk solely based on the technical feasibility of an attack or evaluating a threat scenario as a single unit does not adequately explain the chain of impacts. Dividing the attack into TTPs and considering the likelihood of each action and its impact on the collaborative mission reflects the formation and propagation of actual risks in the MUM-T environment. The comparison results suggest that TTP-based risk assessment, which includes both attack actions and their impacts, is a more suitable approach for highly interdependent collaborative environments such as MUM-T.

5 Discussion

This study analyzed threats associated with collaboration interfaces in the MUM-T environment and proposed a behavior-based risk assessment methodology that integrates the MITRE ATT&CK framework with MCDM techniques. Experimental results demonstrate that the proposed methodology quantitatively reflects the structural characteristics of attack chains and the relative importance of TTPs. Compared to traditional threat-based assessments, it represents these factors in a more systematic and measurable way. However, several limitations remain to be addressed in future research.

The threat scenarios addressed in this study are limited to a few representative cases. While the impact of these threats was analyzed from a functional perspective focusing on collaboration interfaces, the resulting effects and scope of influence may vary depending on factors such as the operational environment, mission type, asset composition, and level of security controls. Conducting a systematic sensitivity analysis of risk calculation results with respect to these variations requires expanding the evaluation scope to include a broader range of threat scenarios. Future research aims to broaden the analysis scope by incorporating the additional scenarios presented in Appendix B. Furthermore, a certain degree of subjectivity may be present in the pairwise comparison process. Appendix A.1 outlines the procedure for deriving comparative values and the criteria for reference selection, and internal cross-checking was conducted. However, the involvement of only two authors is insufficient to substitute for independent verification by multiple experts. Additional expert assessment is required to enhance the validity of the weight calculation results. This study adopts the weighted-sum method as the primary aggregation function due to its interpretability and ease of comparison across methodologies. In MCDM-based evaluations, alternative aggregation methods such as Ordered Weighted Averaging (OWA) and fuzzy aggregation are also available. However, these approaches require additional design elements in the evaluation model, including parameter specification and membership function definition. These requirements introduce unverified assumptions into the evaluation process, which may affect the resulting risk values. The focus of this study is not on the aggregation technique itself. Instead, it aims to validate a methodology that structures collaboration interface-based threats at the behavioral level, identifies risk mitigation elements, and connects them to a quantitative evaluation framework. To achieve this objective, the weighted-sum method was applied due to its reproducibility and interpretive transparency. Sensitivity analysis of TTP weight variations remains a subject for future research.

Future research expands the analysis by constructing additional threat scenarios that reflect diverse operational conditions and asset configurations. It also examines the sensitivity of risk calculation results to variations in TTP weights. The scope further includes automated threat scenario generation using large language models (LLMs) and the development of machine learning-based risk prediction models. LLMs generate large-scale threat scenarios and TTP combinations under diverse MUM-T operational conditions. The corresponding pairwise comparison matrices are accumulated to construct training data. A predictive model is designed to learn common patterns of relative importance among TTPs and to automatically estimate the weights of newly identified threats. The methodology is integrated with a Markov model to establish an adaptive assessment system in which risk dynamically evolves according to the stage of attack

progression. Also, to ensure reliability, duplicate removal and structural constraint validation are conducted. Consistency verification with the ATT&CK framework and expert cross-review are performed in parallel. Hallucination is minimized through a human-in-the-loop structure that applies RAG-based knowledge grounding and prompt constraints.

6 Conclusion

This study proposes a methodology for analyzing and quantitatively assessing security threats in the MUM-T environment, focusing on the collaboration interface, a key point where threats enter and their impacts propagate. To achieve this, the MITRE ATT&CK framework was used to model potential attacks at the collaboration interface on a TTP basis, and MCDM techniques were applied to quantify the relative importance of each TTP. The proposed methodology performed behavior-based risk assessment by integrating the likelihood and impact of each TTP using a weighted-sum approach, thereby reflecting both the feasibility of the attack and its impact on collaborative mission execution.

The application of the proposed methodology to the GPS- and battery-spoofing scenarios revealed that the position on the risk matrix significantly changed compared to those of the NIST SP 800-30 Rev.1 and TARA-based risk assessments, even for the same threat scenario. Although existing methodologies tended to position the risk in relatively high areas because of their comprehensive evaluation at the scenario level, the proposed methodology systematically reflected the likelihood and impact of each TTP, leading to a shift in the risk to a more mitigated position without excessively concentrating it on specific elements. Thus, risk assessment in the MUM-T environments functions not merely as risk classification, but also as decision-making grounds for determining which attack behaviors require prioritized responses against each threat.

This study demonstrated that TTP-based threat modeling and risk-assessment approaches centered on collaboration interfaces reflect the structural characteristics of the MUM-T environments more realistically. The proposed methodology serves as a practical basis for determining the response priorities against various threats occurring in MUM-T.

Acknowledgement: This work was supported by Kyonggi University's Graduate Research Assistantship 2026 and the Challengeable Future Defense Technology Research and Development Program through the Agency for Defense Development (ADD) funded by the Defense Acquisition Program Administration (DAPA) in 2024 (No. 915024201).

Funding Statement: This work was supported by Kyonggi University's Graduate Research Assistantship 2026 and the Challengeable Future Defense Technology Research and Development Program through the Agency for Defense Development (ADD) funded by the Defense Acquisition Program Administration (DAPA) in 2024 (No. 915024201).

Author Contributions: Conceptualization, Gaeul Kim; methodology, Gaeul Kim and Dohoon Kim; formal analysis, Gaeul Kim and Dohoon Kim; investigation, Gaeul Kim; data curation, Gaeul Kim and Dohoon Kim; writing—original draft preparation, Gaeul Kim; writing—review and editing, Gaeul Kim and Dohoon Kim; visualization, Gaeul Kim; supervision, Dohoon Kim; funding acquisition, Dohoon Kim. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Please contact the corresponding author at karmy01@kyonggi.ac.kr.

Ethics Approval: Not applicable.

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

Appendix A TTP-Based Risk Assessment Method Using MCDM

Appendix A.1 Reference Selection and Pairwise Comparison Protocol

The pairwise comparisons conducted in this study were grounded in references that enable objective determination of the relative importance among TTPs, thereby reducing reliance on arbitrary judgment. These references were not used as direct sources of comparison values. Instead, they provided supporting evidence for assessing the technical characteristics and mission-level impact of each attack technique. The literature used to determine pairwise comparison values was selected only when it satisfied the following criteria.

- Specificity of Attack Mechanism: Studies were included when they clearly described the attack execution process, its operational principles within the system, and the vulnerabilities exploited.
- Clarity of Impact: Studies were included when they explicitly explained the specific changes induced by the attack in system behavior.
- Identifiability of Impact Severity: Studies were selected when attack effects were presented through experimental results, simulation metrics, or system performance analysis.
- Operational Environment Relevance: Studies focusing on wireless communication-based UAV operational environments or structurally similar systems were prioritized.

For each representative scenario, at least two references were reviewed. These references were used to cross-validate technical feasibility and scope of impact prior to selection. Based on the selected references, the structural roles of the identified TTPs were analyzed as described in Section 3.2.2. The analysis focused on the functional position of each TTP within the threat scenario. It also examined the changes in system behavior resulting from successful attack execution. In addition, the scope of impact on mission continuity was evaluated. The persistence of the impact and the potential for recovery were also considered. The compiled comparative information was then used to determine dominance relationships among TTPs. The following procedure was applied.

- Compare the structural role of each TTP within the attack chain, including whether it constitutes an essential step or functions as a branching point.
- Assess the uniqueness of that role, including whether the TTP is replaceable or whether its removal would result in the collapse of the attack chain.
- Compare the scope and persistence of the impact on system behavior and operational decision-making in the event of a successful attack, including whether the impact is confined to specific components or extends to the entire mission.

By synthesizing these elements, the relative dominance among the TTPs was first determined. The comparative values were then quantified by mapping them to Saaty's 1–9 scale. The definitions of this scale are presented in Table A1.

The initial comparative values were derived from literature analysis. Subsequent internal cross-reviews ensured consistency of judgment. In cases of disagreement, re-examined to establish consensus values. The final pairwise comparison matrix was adopted only when it satisfied the consistency criterion of $CR < 0.1$.

Table A1: Saaty's fundamental 1–9 scale for pairwise comparison.

Intensity of Importance	Definition
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2, 4, 6, 8	Intermediate values between adjacent judgments

Appendix A.2 Theoretical Assumptions of Pairwise Comparison

The pairwise comparison-based weight calculation method applied in this study follows the fundamental theory proposed by Saaty [14]. The risk problem was decomposed into a hierarchical structure consisting of attack target, attack action, and impact. Accordingly, the following four key assumptions are adopted.

(1) Hierarchical Structure

In this study, risk was hierarchically decomposed into a structure consisting of attack target, attack action, and impact. The top-level objective serves as the evaluation criterion for subordinate elements, and each hierarchical level follows a unidirectional structure. The independence assumed here does not imply complete causal independence among elements. Rather, it refers to structural independence, meaning that no mutual feedback structure exists among elements within the same level. In other words, the importance of one element is not directly determined or modified by other elements at the same hierarchical level. From the perspective of an attack chain, dependencies arise during the execution phase. Certain impacts occur only when specific TTPs precede them. The comparison in this study does not evaluate the temporal sequence of attack execution. It compares the relative contribution of each TTP to collaborative mission execution under a common evaluation criterion. Causal linkages in the execution phase do not prevent independent comparison among TTPs within the same layer. Each TTP is assessed according to its relative contribution to mission impact. This structure satisfies the structural prerequisite of the hierarchical decomposition-based comparison method.

(2) Reciprocity

The pairwise comparison matrix $A = [a_{ij}]$ is constructed as a positive reciprocal matrix. If element i is evaluated as a_{ij} times more important than element j, the reciprocal relationship satisfies the following condition:

$$a_{ji} = \frac{1}{a_{ij}}$$

This condition ensures the mathematical consistency of comparative judgments and is satisfied at the matrix definition stage.

(3) Completeness

For all pairs of elements within the same layer, comparison values are defined. For n elements, every entry a_{ij} of the $n \times n$ comparison matrix is assigned a value, and no comparison omission exists. Completeness serves as a prerequisite for calculating the relative importance of each element through eigenvector analysis. It constitutes a structural requirement for ensuring computability.

(4) Consistency

When complete consistency holds, pairwise comparison judgments satisfy multiplicative transitivity.

$$a_{ik} = a_{ij} \times a_{jk}$$

For example, if element A is twice as important as B, and B is three times as important as C, then A is six times as important as C. When this relationship holds for all element pairs, the matrix satisfies complete consistency. In practical evaluation, perfect transitivity is difficult to achieve. The consistency of the comparison matrix is therefore measured quantitatively. The judgment matrix is adopted only within an acceptable consistency range. In this study, the final matrix was adopted when $CR < 0.1$.

Appendix A.3 Weight Computation Procedure and Results

The TTPs filtered and selected according to the criteria outlined in Section 3.2.2 for each scenario are presented in Table A2. This section outlines the process of constructing the pairwise comparison matrix and calculating the weights for the TTP sets defined in each scenario. This study follows the standard pairwise comparison-based weight calculation procedure without introducing additional transformation processes or computational steps. Consequently, its computational complexity is identical to that of a standard pairwise comparison-based analysis. In pairwise comparison analysis, constructing the comparison matrix for n TTPs requires evaluating each pair of elements. The total number of comparisons is $\frac{n(n-1)}{2}$, resulting in a computational complexity of $O(n^2)$ for matrix construction. Weight calculation and consistency verification involve matrix operations. The maximum eigenvalue of the comparison matrix is computed, from which the CI is derived. The time complexity of this process is generally $O(n^3)$.

Table A2: Identified TTPs for each attack scenario.

Scenario	Identified TTPs (MITRE ATT&CK ID)
GPS Spoofing (S-01)	T1592 (Gather Victim Host Information) T1133 (External Remote Services) T1059 (Command and Scripting Interpreter) T1562 (Impair Defenses) T1036 (Masquerading) T1040 (Network Sniffing) T1046 (Network Service Discovery) T1090 (Proxy) T1565 (Data Manipulation) T1491 (Defacement)
Battery Spoofing (S-02)	T1190 (Exploit Public-Facing Application) T1059 (Command and Scripting Interpreter) T1046 (Network Service Discovery) T1040 (Network Sniffing) T1557 (Adversary-in-the-Middle) T1565 (Data Manipulation) T1489 (Service Stop)

(1) GPS Spoofing Scenario (S-01)

Table A3 presents the pairwise comparison matrix constructed for the TTPs identified in the GPS Spoofing scenario, together with the calculated weights. Each matrix element a_{ij} represents the relative importance of TTP i compared to TTP j in terms of contribution to mission impact. The matrix satisfies the reciprocal condition, and all diagonal elements are set to 1.

Table A3: Pairwise comparison matrix and weight computation results for S-01.

	T1592	T1133	T1059	T1562	T1036	T1040	T1046	T1090	T1565	T1491	GM	Weight	*Aw*	λ_i
T1592	1.000	0.200	0.143	0.333	0.143	0.200	3.000	0.111	0.111	0.333	0.284	0.019	0.206	10.702
T1133	5.000	1.000	0.333	3.000	0.200	3.000	5.000	0.167	0.143	3.000	1.007	0.068	0.761	11.109
T1059	7.000	3.000	1.000	5.000	0.333	3.000	7.000	0.250	0.200	5.000	1.684	0.115	1.236	10.791
T1562	3.000	0.333	0.200	1.000	0.143	0.333	3.000	0.143	0.143	0.333	0.425	0.029	0.303	10.464
T1036	7.000	5.000	3.000	7.000	1.000	5.000	7.000	0.250	0.333	5.000	2.529	0.172	1.929	11.218
T1040	5.000	0.333	0.333	3.000	0.200	1.000	5.000	0.200	0.143	3.000	0.823	0.056	0.608	10.870
T1046	0.333	0.200	0.143	0.333	0.143	0.200	1.000	0.111	0.111	0.200	0.216	0.015	0.159	10.788
T1090	7.000	3.000	3.000	5.000	0.333	5.000	7.000	1.000	0.333	5.000	2.392	0.163	1.742	10.711
T1565	9.000	7.000	5.000	7.000	3.000	7.000	9.000	2.000	1.000	7.000	4.749	0.323	3.400	10.530
T1491	3.000	0.333	0.200	3.000	0.200	0.333	5.000	0.200	0.143	1.000	0.597	0.041	0.436	10.752

The geometric mean (GM) of each row reflects the overall relative dominance of the corresponding TTP compared to all other TTPs. The GM vector serves as an approximation of the principal eigenvector of the comparison matrix. This vector was normalized to derive the weight of each TTP. Subsequently, the weight vector was multiplied by the comparison matrix to compute *Aw*. Each component of *Aw* was divided by the corresponding weight to obtain the consistency vector λ_i. The maximum eigenvalue $\lambda_{\max}$ was estimated from the mean of the consistency vector. The CI and CR were then calculated based on this value. For the GPS Spoofing scenario, $CI = 0.088$ and $CR = 0.059$. The calculated CR satisfied the acceptance criterion < 0.1, and the derived weights were adopted as the final importance scores. Subsequently, seven core TTPs were selected using a cumulative weight threshold of 90%. The same procedure was applied to the selected core TTP set to derive the final weights, as presented in Table A4.

Table A4: Pairwise comparison matrix and weight computation results for selected core TTPs (S-01).

	T1133	T1059	T1036	T1040	T1090	T1565	T1491	GM	Importance	Weight	λ_i
T1133	1.000	0.500	0.333	3.000	0.333	0.200	3.000	0.720	0.076	0.554	7.329
T1059	2.000	1.000	0.333	3.000	1.000	0.250	4.000	1.104	0.116	0.835	7.194
T1036	3.000	3.000	1.000	5.000	2.000	0.333	5.000	2.046	0.215	1.576	7.330
T1040	0.333	0.333	0.200	1.000	0.250	0.143	2.000	0.398	0.042	0.305	7.294
T1090	3.000	1.000	0.500	4.000	1.000	0.333	4.000	1.346	0.141	1.019	7.207
T1565	5.000	4.000	3.000	7.000	3.000	1.000	6.000	3.582	0.376	2.783	7.394
T1491	0.333	0.250	0.200	0.500	0.250	0.167	1.000	0.320	0.034	0.250	7.420

Following the same procedure, $\lambda_{\max}$, CI, and CR were calculated. The resulting values were $CI = 0.052$ and $CR = 0.039$, satisfying the acceptance criterion ($CR < 0.1$) and confirming the consistency of the comparison matrix.

(2) Battery Spoofing Scenario (S-02)

Table A5 presents the results of the pairwise comparison analysis conducted on the TTPs identified in the Battery Spoofing scenario. The analysis followed the same procedure applied in the GPS Spoofing scenario.

Table A5: Pairwise comparison matrix and weight computation results for selected core TTPs (S-02).

	T1190	T1046	T1040	T1557	T1059	T1565	T1489	GM	Importance	Weight	λ_i
T1190	1.000	3.000	2.000	0.333	0.500	0.200	0.200	0.631	0.065	0.464	7.117
T1046	0.333	1.000	0.500	0.167	0.250	0.125	0.125	0.271	0.028	0.200	7.137
T1040	0.500	2.000	1.000	0.250	0.333	0.167	0.167	0.420	0.043	0.308	7.104
T1557	3.000	6.000	4.000	1.000	2.000	0.500	0.500	1.669	0.172	1.216	7.062
T1059	2.000	4.000	3.000	0.500	1.000	0.333	0.333	1.042	0.108	0.761	7.073
T1565	5.000	8.000	6.000	2.000	3.000	1.000	1.000	2.826	0.292	2.061	7.064
T1489	5.000	8.000	6.000	2.000	3.000	1.000	1.000	2.826	0.292	2.061	7.064

For S-02, a comparison matrix was constructed based on the same criteria, and consistency was verified. The calculated values were $CI = 0.015$ and $CR = 0.011$, satisfying the acceptance condition $CR < 0.1$. Applying the 90% cumulative weight threshold, five core TTPs were selected. The results of the pairwise comparison analysis for the selected TTP set are presented in Table A6. For the re-analysis of the core TTP set in S-02, the calculated values were $CI = 0.013$ and $CR = 0.012$, satisfying the acceptance criterion $CR < 0.1$. Accordingly, the consistency of the comparison matrix was confirmed, and the derived weights were adopted as the final importance values.

Table A6: Pairwise comparison matrix and weight computation results for selected core TTPs (S-02).

	T1190	T1557	T1059	T1565	T1489	GM	Importance	Weight	λ_i
T1190	1.000	0.250	0.333	0.143	0.143	0.279	0.043	0.218	5.033
T1557	4.000	1.000	2.000	0.333	0.500	1.059	0.164	0.838	5.092
T1059	3.000	0.500	1.000	0.333	0.333	0.699	0.109	0.549	5.057
T1565	7.000	3.000	3.000	1.000	1.000	2.290	0.356	1.806	5.079
T1489	7.000	2.000	3.000	1.000	1.000	2.112	0.328	1.642	5.006

Appendix A.4 Likelihood and Impact Assessment Criteria

In this study, Likelihood (L_i) and Impact (I_i) were evaluated using a 1–5 scale [26]. The evaluation scores were derived based on explicit assessment criteria rather than arbitrary assignment. These criteria considered the technical characteristics of each TTP and the operational conditions of the scenario. Initial scores were determined through technical analyses and experimental or simulation results reported in relevant literature. The scores were subsequently adjusted to reflect direct verification of attack feasibility and system response within the MUM-T testbed environment constructed in this study. An internal cross-review was then conducted to ensure consistency of judgment. In cases of disagreement, the relevant evidence was re-examined to establish a consensus score.

(1) Likelihood Assessment Criteria

Likelihood does not represent the independent probability of occurrence of a specific TTP. Instead, it reflects the extent to which the TTP contributes to the potential success of an attack. The following factors were comprehensively considered in determining this contribution.

- Technical prerequisites required for attack execution
- Feasibility within wireless communication-based UAV operational environments
- Level of attack complexity and required attacker capability
- Reproducibility demonstrated through experimental or simulation results in existing literature

Scores were assigned according to the following criteria.

- 1: Theoretically possible but subject to significant practical constraints
- 2: Feasible under limited operational conditions
- 3: Achievable but requiring a certain level of technical expertise
- 4: Executable using commonly available tools and standard environments
- 5: Publicly documented and widely reproducible, with high practical likelihood of execution

(2) Impact Assessment Criteria

Impact represents the extent to which a given TTP affects overall mission execution and collaborative operational stability when successfully executed. The evaluation focuses on mission-level ripple effects and persistence, rather than on the mere occurrence of functional failure. The following factors were considered:

- Scope of affected system components
- Duration of operational disruption or performance degradation
- Recovery difficulty and system resilience
- Impact on mission-level decision-making

The impact scores were defined according to the following scale:

- 1: Localized impact with negligible effect on mission execution
- 2: Partial functional degradation with limited mission impact
- 3: Noticeable degradation in mission execution efficiency
- 4: Substantial impact on mission execution
- 5: Mission failure or loss of system control

Appendix B Experimental Setup and Extended Scenarios

Appendix B.1 Experimental Testbed Configuration

All experiments in this study were conducted within an isolated Docker-based Drone Virtual Domain (DVD) environment. ArduPilot SITL and QGroundControl were executed as components integrated within the DVD environment and were not installed as standalone software packages. The attacker executed attack scripts on the host system (Kali Linux) and accessed the containerized DVD environment through a virtual network interface. The overall testbed architecture is illustrated in Fig. A1.

Table A7 summarizes the operating system, container engine, communication stack, and key components of the experimental testbed.

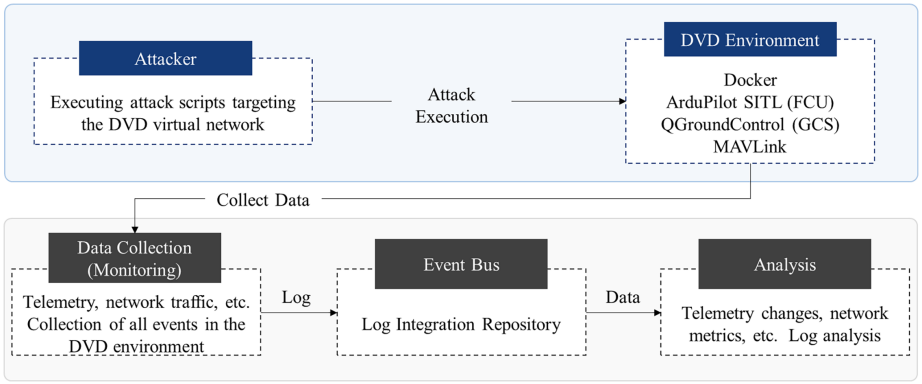


Figure A1: DVD-based experimental testbed architecture.

Table A7: Simulation and experimental environment.

Component	Specification
CPU	AMD Ryzen 9 5900X3D (12C/24T)
GPU	NVIDIA RTX 3080 Ti (12 GB)
RAM	32 GB DDR4
Docker engine	Docker version 29.2.1
Docker OS	Kali Linux 2025.3
UAV platform	Damn Vulnerable Drone (DVD)
ArduPilot	SITL (bundled in DVD)
QGroundControl	integrated in DVD environment
Protocol	MAVLink 2.0

Appendix B.2 Attack Script Pseudocode

This section presents the operational flow of the primary threat scenario described in the main text in pseudocode form. As illustrated in Algorithm A1, GPS spoofing involves repeatedly transmitting packets containing forged MAVLink telemetry messages to the GCS, thereby overwriting the legitimate drone's position information. The attacker continuously injects falsified location data disguised as normal status information by combining HEARTBEAT, GPS_RAW_INT, GLOBAL_POSITION_INT, and ATTITUDE messages.

Algorithm A1: GPS spoofing via forged MAVLink telemetry injection

Input: Target GCS IP address *ip*, MAVLink UDP port *port*
Initialize MAVLink encoder (srcSystem = 1, srcComponent = 1)
while True **do**
  Create **HEARTBEAT** message (masquerade as active quadrotor)
  Create **GPS_RAW_INT** with forged latitude and longitude
  Create **GLOBAL_POSITION_INT** with forged global position
  Create **ATTITUDE** message for state consistency
  Pack messages into MAVLink frames
  Send frames via UDP to *(ip, port)*
end while

Battery spoofing involves repeatedly transmitting packets containing forged BATTERY_STATUS messages to the GCS. This manipulation causes the GCS to interpret the battery level as depleted. As illustrated in Algorithm A2, the attack sets the battery_remaining value to 0. It also artificially inflates the reported consumption rate. These actions trigger an emergency landing or Return-to-Launch (RTL) procedure.

Algorithm A2: Battery spoofing via forged MAVLink BATTERY_STATUS injection

1: **Input:** Target GCS IP address *ip*, MAVLink UDP port *port*
2: Initialize MAVLink encoder (srcSystem = 1, srcComponent = 1)
3: **while** True **do**
  4: Create **BATTERY_STATUS** message
    - Set *battery_remaining* = 0
    - Set *current_consumed* to high value
    - Set *energy_consumed* to high value
    - Set *current_battery* = −1 (unknown/invalid reading)
  5: Pack message into MAVLink frame
  6: Send frame via UDP to *(ip, port)*
7: **end while**

Appendix B.3 Additional Experimental Scenarios

The main body of this study conducted risk assessments focused on GPS spoofing and battery spoofing scenarios. These scenarios serve as representative examples to demonstrate the applicability of the proposed assessment framework. The scope of threats extends beyond the cases discussed in the main text. Table A8 lists the attack scripts implemented in the experimental environment. A total of 37 additional threat scenarios were implemented. These scenarios encompass various collaboration interface-based threats, including network access exploitation, MAVLink message forgery and tampering, command injection, session hijacking, parameter extraction, and firmware analysis and modification.

Table A8: Additional attack scenarios implemented in the testbed environment.

Attack ID	Attack Script	Description
A-1	gps-spoofing	Injects forged GLOBAL_POSITION_INT and GPS_RAW_INT messages to manipulate reported position.
A-2	battery-spoofing	Injects forged SYS_STATUS messages to manipulate battery levels and trigger RTL/LAND behavior.
A-3	satellite-spoofing	Injects forged GPS_RAW_INT messages to manipulate satellite count and fix type.
A-4	attitude-spoofing	Injects forged ATTITUDE messages to manipulate roll, pitch, and yaw values on the GCS.
A-5	vfr-hud-spoofing	Injects forged VFR_HUD messages to manipulate altitude and heading data.
A-6	emergency-status-spoofing	Injects forged STATUSTEXT messages (severity = EMERGENCY) to trigger failsafe states.

(Continued)

Table A8 (continued)

Attack ID	Attack Script	Description
A-7	critical-error-spoofing	Injects forged STATUSTEXT messages (severity = CRITICAL) to display false errors.
A-8	system-status-spoofing	Injects forged SYS_STATUS messages to manipulate sensor health indicators.
A-9	gps-offset-glitching	Applies small positional offsets to induce navigation drift.
A-10	geofencing-attack	Modifies PARAM_SET (FENCE_ENABLE = 0) to disable geofencing restrictions.
A-11	flight-termination	Sends MAV_CMD_DO_FLIGHTTERMINATION to terminate flight immediately.
A-12	return-to-home-point-override	Modifies MAV_CMD_DO_SET_HOME to change the Return-to-Home location.
A-13	mavlink-injection-attack	Injects arbitrary MAVLink command messages (ARM, mode change, reboot).
A-14	waypoint-injection	Injects MISSION_ITEM_INT messages to alter mission waypoints.
A-15	flight-mode-injection	Sends MAVLink SET_MODE commands to change flight mode.
A-16	gps-data-injection	Injects GPS_INPUT messages to supply forged GPS data to EKF.
A-17	wifi-deauth-attack	Sends 802.11 deauthentication frames to disconnect the drone–GCS Wi-Fi link.
A-18	ground-control-station-spoofing	Uses forged HEARTBEAT messages to hijack the C2 session.
A-19	camera-feed-ros-topic-flooding	Floods ROS/camera/image_raw topic to disrupt camera services.
A-20	communication-link-flooding	Floods MAVLink messages to disrupt command transmission.
A-21	wifi-analysis-cracking	Scans Wi-Fi access points and cracks WPA2-PSK keys to gain access to the drone network.
A-22	drone-discovery	Identifies drone systems by scanning for ArduPilot SITL services and MAVLink ports.
A-23	companion-computer-discovery	Detects Companion Computer IP addresses and exposed services (UI, SSH, FTP, RTSP).

(Continued)

Table A8 (continued)

Attack ID	Attack Script	Description
A-24	ground-control-station-discovery	Identifies GCS IP addresses and MAVLink UDP ports.
A-25	packet-sniffing	Captures MAVLink UDP/TCP packets to analyze communication content.
A-26	protocol-fingerprinting	Analyzes MAVLink HEARTBEAT messages to identify protocol version and system ID.
A-27	drone-gps-telemetry-detection	Monitors GLOBAL_POSITION_INT and GPS_RAW_INT messages to detect real-time drone location data.
A-28	flight-log-extraction	Uses LOG_REQUEST_LIST and LOG_REQUEST_DATA to retrieve logs.
A-29	parameter-extraction	Uses PARAM_REQUEST_LIST to extract parameters.
A-30	ftp-eavesdropping	Connects via FTP to download firmware or log files.
A-31	camera-feed-eavesdropping	Subscribes to ROS topics or RTSP streams to capture live footage.
A-32	wifi-client-data-leak	Extracts Wi-Fi client information including MAC addresses.
A-33	mission-extraction	Uses MISSION_REQUEST_LIST and MISSION_REQUEST_INT to extract mission plan.
A-34	companion-computer-bf	Performs brute-force login attempts on web UI.
A-35	companion-computer-takeover	Gains control via successful SSH access.
A-36	camera-gimbal-takeover	Sends MAVLink gimbal control messages to manipulate camera orientation.
A-37	denial-of-takeoff	Blocks ARM commands or manipulates pre-arm conditions.
A-38	firmware-decompile	Reverse engineers firmware binaries to analyze internal logic.
A-39	firmware-modding	Uploads modified firmware to insert backdoors or bypass safeguards.

References

1. JAPCC. Manned-unmanned teaming a great opportunity or mission overload? [Internet]. [cited 2025 Dec 30]. Available from: https://www.japcc.org/articles/manned-unmanned-teaming/.
2. Pandey DK. Manned-unmanned teaming: enhancing lethality. SYNERGY. 2024;3(2):260–79.
3. Niedzielski T, Jurecka M, Mizinski B, Pawul W, Motyl T. First successful rescue of a lost person using the human detection system: a case study from Beskid Niski (SE Poland). Remote Sens. 2021;13(23):4903. doi:10.3390/rs13234903.

4. Stasik J, Szandala T. An autonomous drone for avalanche search and rescue: integrating ArduPilot and tracking-beacon detection. IEEE Access. 2025;13(122):130758–69. doi:10.1109/ACCESS.2025.3585245.
5. Al-Husseini M, Wray KH, Kochenderfer MJ. Hierarchical framework for optimizing wildfire surveillance and suppression using human-autonomous teaming. J Aerospace Inf Syst. 2024;21(10):790–811. doi:10.2514/1.I011368.
6. Boroujeni SPH, Razi A, Khoshdel S, Afghah F, Coen JL, O'Neill L, et al. A comprehensive survey of research towards AI-enabled unmanned aerial systems in pre-, active-, and post-wildfire management. Inf Fusion. 2024;108(4):102369. doi:10.1016/j.inffus.2024.102369.
7. NASA. Man UnManned Teaming (MUMT) (or the more acceptable-human autonomy teaming) in the civil domain [Internet]. [cited 2025 Dec 30]. Available from: https://ntrs.nasa.gov/citations/20210022211.
8. Yang H, Guo Y, Guo Y. Fault-tolerant security-efficiency combined authentication scheme for manned-unmanned teaming. Comput Secur. 2024;146:104052. doi:10.1016/j.cose.2024.104052.
9. Naval Postgraduate School. UxS Manned/unmanned secure teaming [Internet]. 2022 [cited 2025 Dec 30]. Available from: https://nps.edu/documents/113838019/133887630/Hale_UxS+Manned_Unmanned+Secure+Teaming+_Quad_2022.pdf/7360091b-552a-975e-8ba0-78d3f32e8a9f?t=1639082740562.
10. Ranjan RK. Manned–unmanned teaming: changing paradigms of warfare. Defence Diplomacy J. 2025;14(2):87–98.
11. Woudenberg M, Waltensperger GM, Shideler T, Franke J. Systems engineering of autonomy: frameworks for MUM-T architecture. J Defense Syst Inf Anal Center. 2020;7(3).
12. Yasar H, Bahtiyar S. Secure communication for MUM-T: a blockchain and lightweight cryptography framework. In: 17th International Conference on Security of Information and Networks (SIN). Piscataway, NJ, USA: IEEE; 2024. p. 1–8.
13. MITRE. MITRE ATT&CK [Internet]. [cited 2025 Dec 30]. Available from: https://attack.mitre.org/.
14. Saaty TL. Decision making with the analytic hierarchy process. Intl J Services Sci. 2008;1(1):83–98. doi:10.1504/ijssci.2008.017590.
15. Kasperczyk N, Knickel K. Analytic hierarchy process (AHP) [Internet]. IfLS. 2022 [cited 2025 Dec 30]. Available from: https://www.iied.org/20781g.
16. Sathaye H, Strohmeier M, Lenders V, Ranganathan A. An experimental study of GPS spoofing and takeover attacks on UAVs. In: 31st USENIX Security Symposium (USENIX Security 22). Berkeley, CA, USA: USENIX Association; 2022. p. 3503–20.
17. Li D, Song HH. GPS spoofing on UAV simulation using ardupilot. In: 2025 International Wireless Communications and Mobile Computing (IWCMC). Piscataway, NJ, USA: IEEE; 2025. p. 114–9. doi:10.1109/iwcmc65282.2025.11059556.
18. Desnitsky V, Kotenko I. Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. Simul Model Pract Theory. 2021;107:102244. doi:10.1016/j.simpat.2020.102244.
19. Dixit B, Ananthapadmanabhan A, Thahsin A, Pathak S, Kasbekar GS, Maity A. A novel cipher for enhancing MAVLink security: design, security analysis, and performance evaluation using a drone testbed. IEEE Open J Commun Soc. 2025;6(1):9027–51. doi:10.1109/OJCOMS.2025.3621318.
20. ISO/SAE 21434. Road vehicles—cybersecurity engineering. Geneva, Switzerland: International Organization for Standardization; 2021.
21. NIST. Guide for conducting risk assessments (SP 800-30 Rev. 1) [Internet]. [cited 2025 Dec 30]. Available from: https://csrc.nist.gov/pubs/sp/800/30/r1/final.
22. OWASP. OWASP risk rating methodology [Internet]. [cited 2025 Dec 30]. Available from: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.
23. Cui Z, Guan K, Briso-Rodríguez C, Ai B, Zhong Z, Oestges C. Channel modeling for UAV communications: state of the art, case studies, and future directions. IEEE Wirel Commun. 2021;28(1):65–71. doi:10.1109/MWC.001.2000213.
24. Khan NA, Jhanjhi NZ, Brohi SN, Almazroi AA, Almazroi AA. A secure communication protocol for unmanned aerial vehicles. Comput Mater Contin. 2022;70(1):601–18. doi:10.32604/cmc.2022.019419.
25. Manesh MR, Kaabouch N. Cyber-attacks on unmanned aerial system networks: detection, countermeasure, and future research directions. Comput Secur. 2019;85(3):386–401. doi:10.1016/j.cose.2019.05.003.

26. Pandey GK, Gurjar DS, Nguyen H, Yadav S. Security threats and mitigation techniques in UAV communications: a comprehensive survey. IEEE Access. 2022;10:112858–97. doi:10.1109/ACCESS.2022.3215975.
27. Abo-Alian A, Youssef M, Badr NL. A data-driven approach to prioritize MITRE ATT&CK techniques for active directory adversary emulation. Sci Rep. 2025;15(1):27776. doi:10.1038/s41598-025-12948-x.
28. Rashid SMZU, Alam MM, Montasir I, Haq A. Risk-based MITRE TTP scoring for proactive cyber threat prioritization and response. In: ICSCA '25: Proceedings of the 2025 14th International Conference on Software and Computer Applications. New York, NY, USA: ACM; 2025. p. 72–6.
29. Repetski EJ, Sarkani S, Mazzuchi T. Applying the analytic hierarchy process (AHP) to expert documents. Int J Anal Hierarchy Process. 2022;14(1):919. doi:10.13033/ijahp.v14i1.919.
30. Aleks N. Damn vulnerable drone [Internet]. 2025 [cited 2025 Dec 30]. Available from: https://github.com/nicholasaleks/Damn-Vulnerable-Drone.git.