

Article

AFAPS: An Efficient ECC-Based Authentication Framework for Autonomous Airdrop Parachute Systems

Burak Civelek ^{1,*}  and Yasin Genc ² ¹ Department of Electrical-Electronic Engineering, Ostim Technical University, 06374 Ankara, Türkiye² Department of Electrical-Electronic Engineering, Gazi University, 06560 Ankara, Türkiye;
yasin.genc@gazi.edu.tr

* Correspondence: 200101010@sivas.edu.tr

Abstract

Airdrops with autonomous ram-air type parachutes are increasingly important in today's unconventional warfare conjuncture and humanitarian aid operations. However, there are fundamental issues to be considered by operators or decision makers as to its utilization in the theatre. It is inevitable that new threats will arise with the increase in technology. Therefore, cyber defense elements for air supply should be secured for guided parachute systems that have the ability to glide through long distances. Some of these implied cyber-attacks could target sensitive information (identity, location, etc.) carried by guided parachutes, which are basically unmanned aerial vehicles, and deviate the system by taking over the routing control. The capture of flight information could lead to the disclosure of such covert operations, or at least lead to unexpected complications such as unauthorized airspace violations. Due to various adverse situations that may occur, ensuring the cybersecurity of the parachute payload system both in flight and on the ground has always been an important research topic. In this study, the concept of information replenishment with autonomous parachute systems is introduced to the literature and the cybersecurity of the system is detailed. Specifically, an efficient, lightweight, and pairing-free Elliptic Curve Cryptography (ECC)-based authentication scheme is proposed to secure the system. Considering the resource-constrained nature of autonomous parachute platforms, the proposed scheme is designed to ensure robust security with minimal computational and communication overheads. Furthermore, a security evaluation of the proposed scheme is performed. Although ECC-based authentication protocols have been widely investigated for UAV and IoT systems, this study is, to the best of our knowledge, the first to adapt a lightweight authentication framework to the cybersecurity requirements of autonomous ram-air parachute systems.

Academic Editor: Aryya
Gangopadhyay

Received: 15 June 2026

Revised: 14 July 2026

Accepted: 20 July 2026

Published: 24 July 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: airdrop; authentication scheme; cybersecurity; precision-guided system

1. Introduction

Airdrops are a replenishment method used to rapidly deliver essential supplies to military units or people in need during emergency situations and humanitarian aid operations when highway or other transportation systems cannot be used [1]. The most significant limitation of airdrops is the vulnerability of the aircraft to enemy air defense weapons [2]. To prevent this deficiency, operations should be carried out from an altitude as high as possible and from a horizontal distance as far from the theatre as possible. Although airlift, for the most part, is a supply transportation method, it can also be used to carry valuable

information to troops, depending on the necessities of the operation [3,4]. A battlefield is a complex situation where all eventualities must be considered. Information may need to be transmitted to the relevant group in situations where communication channels and devices are unusable. In cases where information needs to be delivered to an area accessible only by air, parachute systems will be needed as a means of delivery that can avoid detection by enemy air defense systems. In this study, the concept of information replenishment with autonomous parachute systems is introduced to the literature. This information can be details of the next operation or mission, newly acquired intelligence, or a modified evacuation plan.

With the maneuvers that can be performed through control of the parachute control ropes by means of motors, trajectory correction can easily be made according to the desired target distance [1,5]. In this system, the Airborne Guidance Unit (AGU) is mounted between the main parachute and the payload, and connected to the steering ropes of the parachute. By pulling in and releasing the steering ropes, the shape of the parachute changes, and so the course of the parachute and the glide ratio are changed. The glide ratio is the covered horizontal distance divided by the change in altitude [6]. Braking may be performed by pulling both of the steering ropes at the same time, as well [7,8]. The highest glide rate of a ram-air type parachute used in military operations is 1/4 [9]. In this context, the highest altitude and the furthest horizontal distance to be covered should be calculated according to the average altitude winds and target point wind direction and strength, and the operation should be carried out within these upper limits [10]. Many companies have made their own designs in order to meet the needs of countries for guided airdrop parachutes [11–13].

In the parachute system, the concept of cybersecurity is expected to come to the fore as much as physical security. With the rapid advancement of the Internet of Things (IoT) [14–16], and the integration of high-speed, low-latency 5G mobile communication technologies [16–18], the use of Unmanned Aerial Vehicles (UAVs) is becoming widespread [15,19]. Since these parachute systems rely on embedded micro-controllers (such as the ESP32 module) for autonomous guidance and IoT-based communication, they become highly vulnerable to cyber threats. Security schemes are designed for the security of communication in unmanned aerial vehicles [20–22]. Similar to unmanned aerial vehicles, the parachute system also has a number of security requirements. Privacy and security problems in unmanned aerial systems are increasing with new generation technologies [22–24]. To prevent this problem, authentication schemes based on cryptographic methods, such as Elliptic Curve Cryptography (ECC), are widely used [25,26]. These schemes are designed based on cryptographic protocols and aim to ensure privacy and security in unmanned aerial vehicles [22,27–30]. A potential cyber-attack targeting the AGU could hijack the steering control or cause the leakage of sensitive operational data carried via information replenishment.

In this paper, a novel efficient, lightweight, and pairing-free authentication scheme is designed to ensure privacy and security in the parachute system. This design is based on elliptic curve cryptography (ECC) due to its efficiency and effectiveness [31,32]. Considering the resource-constrained nature of parachute embedded hardware, the proposed framework is optimized to provide robust security with minimal computational and communication overhead. In addition, the unique security requirements for parachute systems were determined, and a security evaluation of the proposed scheme is performed to verify whether it satisfies these criteria.

The rest of the paper is organized as follows: Section 2 presents the related studies in the literature. Section 3 outlines the contributions. Section 4 presents the basic definitions of the precision-guided airdrop system, hardware, cybersecurity, and elliptic curve cryptography. Section 5 presents the security requirements and cyber-attacks. Section 6 presents the proposed AFAPS authentication scheme. Section 7 provides the security evalu-

ation, including the adversary model, informal security analysis, and BAN Logic-based formal analysis. Section 8 presents the performance analysis. Finally, Section 9 concludes the paper.

2. Related Work

The trajectory planning of guided airdrop parachutes and the analysis of their gliding fashion are made through modeling since real airdrops are costly and difficult [33]. Parachute systems in the first ever models were introduced as 3-DOF (Degrees of Freedom). In these models, movements in three axes are modeled and the effects of horizontal and vertical velocities are ignored. Forward movement, horizontal movement and rotational movements of the system are modeled. Then, 4-DOF models were made in which the change of descent and the descent of the system as a whole were added according to the shape change experienced when the system was rotated [34]. In 4-DOF modeling, the rotational movement of the forward and horizontal axes is defined as the dive angle of the payload and parachute. In 6-DOF modeling, three (x-y-z) Cartesian coordinates and three (yaw-pitch-roll) Euler angles were used. In 3 DOF, 4-DOF and 6-DOF models, the parachute and payload are considered as a single object [35,36]. In the later models, the payload and the parachute were considered as two different objects, and the movements of the center of gravity in the middle of the payload and parachute were also taken into consideration. In this way, models with 7 DOF, 8 DOF and 9 DOF were tested [37]. Although guided airdrop parachute systems are generally used in studies with 6-DOF modeling, modeling studies have been performed involving up to 12 or even 15 degrees of freedom [38,39].

While the physical modeling and aerodynamic analyses of autonomous parachute systems have been extensively investigated, the integration of digital controllers and IoT-based communication modules has exposed these platforms to critical cyber vulnerabilities. Particularly with the introduction of the information replenishment concept, securing the communication and data integrity of guided parachutes against malicious interventions has become just as vital as their physical stability. Consequently, authentication schemes come to the fore in the evaluation of the parachute system or unmanned aerial vehicles in terms of cybersecurity [25,26,28–30,40–44].

An ECC-based secure authentication scheme for unmanned aerial vehicles has been proposed by Ever [20]. A security analysis was performed to prove the security of the proposed scheme. Hussain et al. [40] proposed an authentication scheme using ECC for drones. The security and performance evaluation has been carried out in detail. For this purpose, ROM (Random Oracle Model) security analysis and comparison with other existing schemes have been performed. Son et al. [41] stated the importance of unmanned aerial vehicles in intelligent transport systems and proposed a blockchain-based authentication scheme. The security analysis of the proposed scheme is performed with BAN logic and the AVISPA simulation tool. In addition, its performance and security are compared with other existing schemes. Li et al. [42] propose a lightweight identity-based authentication scheme. This scheme uses ECC as a cryptographic method. It is claimed that the proposed scheme achieves favorable results when compared in efficiency with traditional authentication schemes in unmanned aerial vehicles. Alladi et al. [43] proposed a lightweight mutual authentication scheme based on Physical Unclonable Functions (PUFs). This scheme is also modelled to enable UAV-UAV communication. The security of the proposed scheme against various cyber attacks is analysed. Nyangaresi et al. [44] proposed a provably secure session key agreement scheme for UAVs. In order to show the efficiency of the proposed scheme, the bandwidth is calculated and compared with the bandwidths of the existing schemes. Addressing the security of highly mobile and resource-constrained nodes, Genc

et al. [45] proposed a new efficient, lightweight, and pairing-free certificateless conditional privacy-preserving authentication scheme (ELCPAS) based on ECC for the Internet of Vehicles (IoV). The proposed scheme performs batch message verification to minimize computational delays while ensuring robust security. In another study, Genc et al. [46] designed a novel pairing-free identity-based privacy-preserving anonymous authentication scheme (NIBPA) for vehicle-to-vehicle (V2V) communication. The comprehensive security and performance evaluations in these studies prove that pairing-free ECC architectures are highly effective in platforms with limited processing power.

In recent literature, a significant portion of these schemes focuses on Unmanned Aerial Vehicles (UAVs) and Internet of Drones (IoD) ecosystems. Khan et al. [47] proposed a certificate-based ring signcryption scheme for securing UAV-enabled private edge computing systems. Lee and Lee [25] designed a lightweight mutual authentication and session key agreement protocol specifically tailored for UAV roaming in multi-fog tactical networks. To secure UAV-assisted Internet of Vehicles (IoV) infrastructures, Choi et al. [26] developed a Physical Unclonable Function (PUF)-based lightweight authentication scheme. Furthermore, Nyangaresi et al. [28] proposed a cost-effective authentication protocol integrating PUF and Elliptic Curve Cryptography (ECC) for secure IoD communication. Emphasizing the critical security requirements of military IoD operations, Choe and Kang [29] introduced a holistic security framework encompassing an ECC-based authentication protocol. Focusing on drone-to-drone communication within the Internet of Autonomous Things, Shariq et al. [30] developed a provably secure and reliable privacy-preserving authentication scheme. Addressing the vulnerabilities of resource-constrained IoT networks, Alzahrani [48] proposed a verifiably secure and lightweight device-to-device (D2D) authentication protocol. Additionally, Zhang et al. [49] introduced an ECC-based three-factor authentication protocol designed to provide session key leakage resilience in the IoD ecosystem. Liu et al. [50] proposed a Physical Unclonable Function (PUF)-based system authentication protocol (UAP) to enable secure UAV-assisted relay communication. Chauhdary et al. [51] proposed a mutual authentication protocol that combines PUFs with an enhanced logistic map. Korkuc et al. proposed an access control scheme for IT [52] followed by a blockchain-based secure access control scheme to protect OT/IT network infrastructures [53], and also proposed secure schemes for the aircraft's blackbox [54] and vehicular networks [55]. The proposed design secures the challenge-response pairs against modeling and eavesdropping attacks, providing a robust and practical solution for nodes with limited computational power. Arachchige et al. [56] presented an integrated cybersecurity framework for V2V and autonomous electric vehicle communications, addressing major cyber threats such as spoofing, replay, jamming, and DoS attacks through threat assessment, vulnerability analysis, cryptographic techniques, secure protocols, and continuous monitoring mechanisms. Yapici and Abut [57] developed a secure IoT-based autonomous electric taxi framework that combines deep learning-based travel and charging time prediction with multi-layer cybersecurity controls including IP authentication, TLS encryption, mutual authentication, and secure OCPP validation. Wang et al. [58] designed an ECC-based authentication protocol for dynamic electric vehicle charging systems, using PUF and ECDLP mechanisms to provide secure vehicle-RSU authentication, privacy protection, forward secrecy, and resistance against common network attacks. El-Hajj [59] investigated the integration of Digital Twins with Intrusion Detection Systems for securing IoT-based cyber-physical infrastructures. The study showed that combining real-time Digital Twin monitoring with IDS-based attack detection can provide a holistic security perspective by analyzing both network-level threats and system resource impacts during cyberattacks. Madububa Mbachu et al. [60] developed a PUF-based privacy-aware authentication scheme for autonomous vehicles in IoV environments, demonstrating that hardware acceleration can reduce computational and

communication overhead while improving authentication security. Elhadad and Gebali [61] developed a PUF-based mutual V2I authentication protocol for multi-hop vehicular networks, providing lightweight authentication, anonymity, forward secrecy, and resistance against replay, impersonation, and man-in-the-middle attacks. Kim [62] introduced an ECC-based lightweight three-party authenticated key exchange protocol for the Internet of Drones networks, demonstrating efficient communication overhead and formal resistance against common attacks such as MITM and impersonation. Zou et al. [63] developed an edge-assisted certificateless aggregated signcryption scheme for VANETs, aiming to improve authentication, privacy protection, conditional traceability, and computational efficiency in resource-constrained vehicular communication environments. Recently, integrated sensing and communication (ISAC) frameworks have also attracted significant attention in autonomous UAV systems. Wu et al. [64] proposed a camera-cooperative ISAC framework for multimodal non-cooperative UAV sensing, demonstrating the growing importance of integrating sensing, communication, and trustworthy information exchange in autonomous aerial platforms. Semenov et al. [65] investigated the protection of Automatic Dependent Surveillance–Broadcast (ADS-B) data for unmanned aerial vehicles, emphasizing the security of identification and communication-related information in airborne platforms. Their study highlights the importance of protecting navigation and identification data, which is also essential for autonomous parachute systems operating in mission-critical environments. These developments further highlight the necessity of secure authentication mechanisms for next-generation autonomous airborne systems.

Despite the extensive cybersecurity research on UAVs, IoD, and IoV networks in the literature, there is currently no study directly addressing the cybersecurity of autonomous parachute systems. Therefore, this study is the first to introduce a specific authentication framework tailored for the unique operational and resource-constrained nature of autonomous ram-air parachutes.

3. Contributions

In this paper, we propose a novel authentication scheme for precision-guided airdrop systems, considering privacy and cybersecurity. The main contributions of this paper are as follows.

- (1) A new kind of usage field for airdrop has been proposed. With this new concept, called information replenishment, precision-guided airdrop systems can be used to transport information.
- (2) With the widespread use of precision-guided airdrop systems in the operation area, the cybersecurity of the transported material should be considered as well as the physical security. In this paper, this problem has been addressed and solution proposals have been emphasized.
- (3) A secure authentication scheme has been designed to ensure the security of the parachute system. This was done to take precautions against cyber attacks on our parachute system.
- (4) The security requirements in our parachute system have been determined. It is proved that the proposed authentication scheme meets these security requirements.
- (5) Considering the resource-constrained hardware of embedded parachute guidance units (e.g., limited battery and processing power), a lightweight and pairing-free Elliptic Curve Cryptography (ECC)-based authentication scheme is designed to ensure robust security with minimal computational and communication overhead.

4. Basic Definitions

4.1. Precision-Guided Airdrop System

A standard guided parachute system is made up of three main parts: the dome of the parachute, the steering control unit and the payload being transported [66]. Due to being controlled by steering lines, a ram air type parachute dome is preferred [67]. The ram air dome has two layers—the upper and lower layers. Nylon fabric with low permeability is used in these layers. There are cells that control the airflow in the space between the top and bottom layers. The attacking side of the wing is left open for air to fill the cells. Since the back of the wing is closed, the air entering the cells stays inside and the wing remains in a robust shape. The air is distributed homogeneously through the holes between the cells. In this way, the parachute maintains its balance. By pulling the steering lines attached to the back side of the wing, the standard shape of the parachute is changed and the parachute can be turned to the desired orientation [68]. In intelligent systems, the steering lines are pulled by the motors in the command and control unit and the parachute is guided unmanned [69,70]. This unit with command motors and direction-finding sensors is called an Airborne Guidance Unit (AGU). The AGU is mounted between the parachute's dome and the load transferred. One of the guided airdrop parachutes is shown in Figure 1.

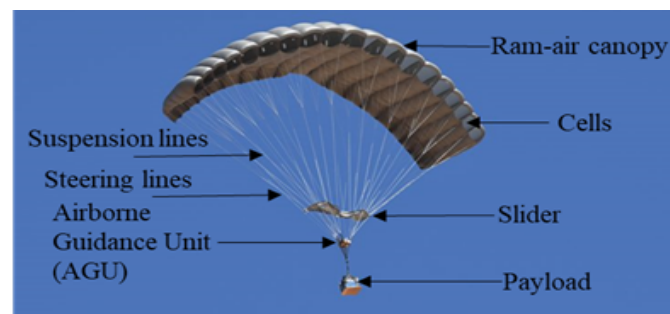


Figure 1. Precision-guided airdrop parachute components.

4.2. Model of the Parachute

In this study, the most preferred 6-DOF parachute models were used. The kinematic equations of the parachute-load system can be described as in Equations (1) and (2).

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = [T_{IB}]^T \begin{pmatrix} u \\ v \\ w \end{pmatrix} \quad (1)$$

$$\begin{pmatrix} \dot{\phi} \\ \dot{\theta} \\ \dot{\psi} \end{pmatrix} = \begin{pmatrix} 1 & \sin \phi \tan \theta & \cos \phi \tan \theta \\ 0 & \cos \phi & -\sin \phi \\ 0 & \sin \phi / \cos \theta & \cos \phi / \cos \theta \end{pmatrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix} \quad (2)$$

In order to create a dynamic model of the parachute, the forces and moments affecting the system must be found. By using Euler angles (roll, pitch, and yaw), rotations around the x, y, and z axes can be defined with individual matrices. These matrices are shown separately in Equations (3)–(5).

$$R_{\sigma x}(\phi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \phi & \sin \phi \\ 0 & -\sin \phi & \cos \phi \end{pmatrix} \quad (3)$$

$$R_{\sigma y}(\theta) = \begin{pmatrix} \cos \theta & 0 & -\sin \theta \\ 0 & 1 & 0 \\ \sin \theta & 0 & \cos \theta \end{pmatrix} \quad (4)$$

$$R_{\sigma z}(\psi) = \begin{pmatrix} \cos \psi & \sin \psi & 0 \\ -\sin \psi & \cos \psi & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (5)$$

T_{IB} is the equation matrix of rotation. This is obtained by multiplying the individual rotation matrices.

$$x = \begin{pmatrix} \cos \theta \cos \psi \\ \sin \phi \sin \theta \cos \psi - \cos \phi \sin \psi \\ \cos \phi \sin \theta \cos \psi + \sin \phi \sin \psi \end{pmatrix} \quad (6)$$

$$y = \begin{pmatrix} \cos \theta \sin \psi \\ \sin \phi \sin \theta \sin \psi + \cos \theta \cos \psi \\ \cos \phi \sin \theta \sin \psi - \sin \theta \cos \psi \end{pmatrix} \quad (7)$$

$$z = \begin{pmatrix} -\sin \theta \\ \sin \phi \cos \theta \\ \cos \phi \cos \theta \end{pmatrix} \quad (8)$$

$$T_{IB} = \begin{pmatrix} x & y & z \end{pmatrix} \quad (9)$$

The aerodynamic force (F_{aero}) acting on the parachute is defined in terms of aerodynamic derivatives. The equation is defined in Equation (10).

$$F_{aero} = 1/2\rho V^2 S C_w^b \begin{pmatrix} -C_D \\ C_Y \\ -C_L \end{pmatrix} \quad (10)$$

where ρ is air density; V is air velocity; S is dome area; b is wing span; C is aerodynamic chord; and C_L , C_D and C_Y are coefficients of lift, drag and side force.

The aerodynamic moment M_{aero} acting on the parachute is defined in terms of aerodynamic derivatives. The equation is defined in Equation (11).

$$M_{aero} = 1/2\rho V^2 S \begin{pmatrix} bC_l \\ cC_m \\ bC_n \end{pmatrix} + rx F_{aero} \quad (11)$$

where C_l , C_m , C_n are the rolling, pitching, and yawing coefficients of motion, and r is the distance from the center of gravity to the aerodynamic reference point.

The 6-DOF dynamics model defines the cyber-physical operating context of the autonomous ram-air parachute system by describing its flight state, trajectory evolution, and guidance behavior during mission execution. Although the model is not directly used as a cryptographic primitive, it identifies the mission-critical information that must be protected during communication, such as the mission message $message_x$, the desired impact

point DP_x , and the information-replenishment payload $Info_x$. In the proposed security framework, these data are included in the encrypted payload as

$$M_x = message_x \parallel DP_x \parallel Info_x \parallel T_x \parallel Seq_x$$

and protected using an ECDH-derived AES-GCM encryption layer. Thus, the dynamics model provides the physical basis of the protected mission information, while the proposed cryptographic mechanism ensures its authentication, integrity, freshness, and confidentiality. Moreover, the 6-DOF model can support trajectory-consistency verification and kinematic anomaly detection against GPS spoofing, trajectory manipulation, and abnormal flight behavior.

4.3. Hardware

Based on the operational environment defined by the autonomous parachute dynamics model, the proposed authentication framework protects mission-critical communication exchanged between the parachute and the control station.

The rollers controlling the steering ropes are driven by two independent motors. Motors are powered by 24 Volt and have a rate of 55 RPM (revolutions per minute). The idle operating current is 1 A, and the strain current is 7 A at most. The rated load torque is 25 kg/cm. 12 V, 6 A dry batteries were chosen as the power source. The system, which works with at least two dry batteries connected in series, has an area where 10 batteries can be placed. In order to minimize the possibility of the ropes tangling and to avoid creating unnecessary volume, the guidance system is designed discreetly. Thus, the guiding rollers could be placed exactly at locations as remote as applicable.

Each motor is driven separately by the IBT-2 BTS7960B motor driver. As the processor, the ESP32 module (Espressif Systems, Shanghai, China) is preferred because it has an embedded Wi-Fi module, has an adequate number of legs for the system, can perform operations involving floating points (processing with decimal numbers), and has a processing speed of 160 MHz.

Additionally, a 9-axis CJMCU-055 precision accelerometer–gyroscope–magnetic sensor, a NEO-7M GPS sensor (u-blox AG, Thalwil, Switzerland) for position determination, an MS5803-01BA altimeter sensor, a DS3231 real time clock sensor, a micro SD card adapter, a current meter and two KY040 rotary encoders are used. A 24C32 eeprom module is employed to prevent data that need to be written very frequently, such as the encoder position, from damaging the SD card. The processor communicates with the GPS sensor via the UART protocol, and with the accelerometer, altitude sensor, clock, SD card and eeprom module via I2C protocol. Position data received from encoder sensors are provided by the digital reading of pins. The current meter is read analogously. Embedded system software is developed in C++ software language and Visual Studio Code version 1.128.1 (Microsoft Corporation, Redmond, WA, USA).

4.4. Cybersecurity

Today, security in critical infrastructures has become a very important issue. In particular, cybersecurity causes significant problems in critical infrastructures. In order to ensure the security of a system, the concept of cybersecurity, as well as physical security, should be examined in detail. In this paper, a new authentication scheme is designed by considering the cybersecurity of the parachute system. Authentication schemes are widely used to ensure the security of the communicating parties. With the IoT, many devices are included in the same network system and communicate with each other. Malicious devices in the network system pose a security risk. Authentication schemes are used to eliminate this risk, particularly in resource-constrained IoT systems where secure communication

and gateway protection are fundamental security requirements [71]. In the proposed authentication scheme, elliptic curve cryptography is used as a cryptography method.

4.5. Elliptic Curve Cryptography

Elliptic curve cryptography is a public key-based cryptography system that is widely used today. In a public-key cryptography system, there are two keys: a public key, which is available to everyone, and a private key, which is available only to the user. Elliptic curve cryptography has some advantages over other cryptography methods. In particular, it is highly preferred in resource-constrained devices thanks to its high security with short key size and features such as low bandwidth and low storage. The basic concepts of elliptic curve cryptography are given below [72].

ECC is defined over the finite field $\mathbb{F}_p$. The elliptic curve E equation is defined as in Equation (12). According to the values of a and b in this equation, the elliptic curve to be formed varies.

$$E : y^2 = x^3 + ax + b \pmod{p}, \quad (12)$$

where p is a large prime number and $a, b \in \mathbb{F}_p$. The choice of the elliptic curve used in cryptographic systems should be over finite fields. The a and b values used in the ECC equation must satisfy Equation (13). If this condition is not fulfilled, a and b values are selected again.

$$4a^3 + 27b^2 \neq 0 \pmod{p} \quad (13)$$

The points on the elliptic curve are obtained by finding the x and y values according to Equation (12). The elliptic curve is constructed by selecting a and b values of -1 and 0 , respectively, and is given in Figure 2.

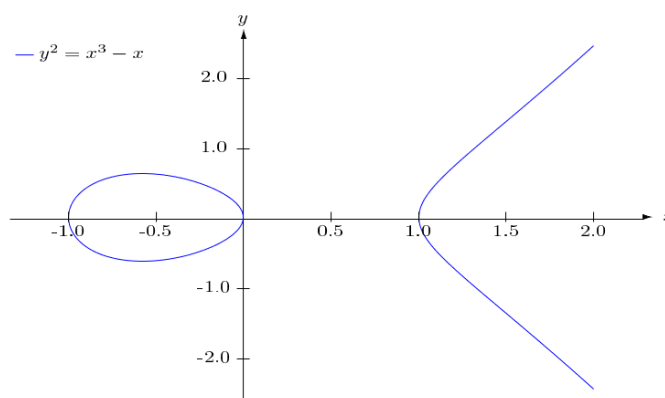


Figure 2. $y^2 = x^3 - x$ elliptic curve.

The security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP). As seen in Equation (14), even if the points P and Q on the elliptic curve are known to any malicious person, it is very difficult to calculate the private key value denoted by k .

$$Q = x \cdot P \quad (14)$$

In ECC, there are basic mathematical operations such as point addition, point doubling and scalar multiplication. Let the elliptic curve E be defined over a prime field $\mathbb{F}_p$ and have two different points, $P(x_1, y_1)$ and $Q(x_2, y_2)$. The line drawn to connect the points intersects the elliptic curve at a third point. Another point, which is the addition of the

points, is found by taking the symmetry of this point with respect to the x-axis ($P + Q = R$). The geometric addition on a finite prime field is shown in Figure 3.

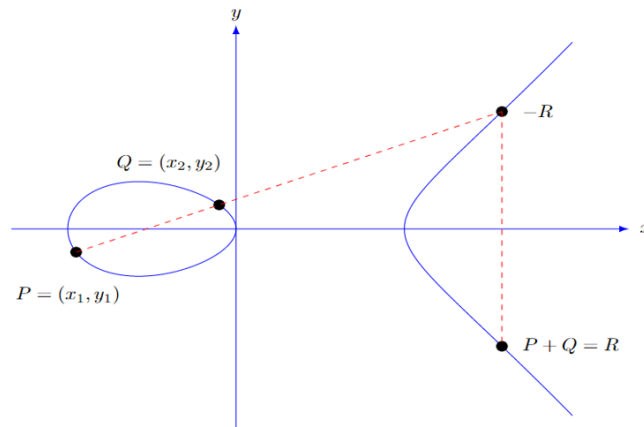


Figure 3. Addition on an elliptic curve ($P + Q = R$).

The addition on the elliptic curve is also performed algebraically. In the point addition performed in Equation (15), x_3 and y_3 are found.

$$R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2) \quad (15)$$

$$x_3 = \lambda^2 - x_1 - x_2 \quad (16)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (17)$$

where λ is calculated as in Equation (18).

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad (18)$$

Point doubling is the process of adding a point P on an elliptic curve with itself ($P + P = 2 \cdot P = R$). The point doubling process is shown geometrically in Figure 4.

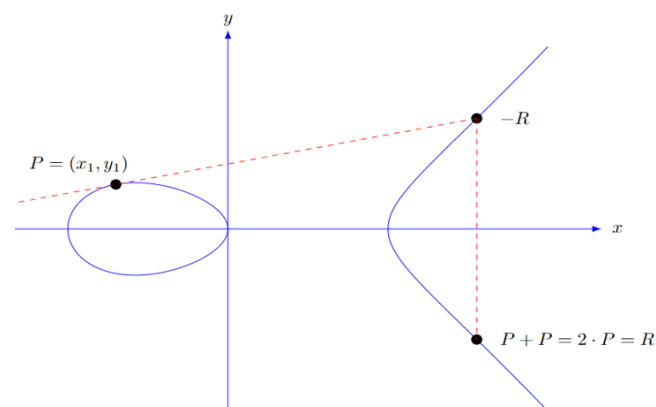


Figure 4. Point doubling on an elliptic curve ($P + P = 2 \cdot P = R$).

The point doubling on the elliptic curve is also performed algebraically. In the point doubling performed in Equation (19), x_2 and y_2 are found respectively.

$$P(x_1, y_1) + P(x_1, y_1) = 2 \cdot P = R(x_2, y_2) \quad (19)$$

$$x_2 = \lambda^2 - 2x_1 \quad (20)$$

$$y_2 = \lambda(x_1 - x_2) - y_1 \quad (21)$$

where λ is calculated as in Equation (22).

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad (22)$$

The operation performed by multiplying the point on the elliptic curve by k is called scalar multiplication. To perform this operation, the point P is added to itself k times, as in Equation (23).

$$k \cdot P = \underbrace{P + P + P \dots + P}_k \quad (23)$$

5. Security Requirements and Cyber Attacks

In this section, security requirements and cyber attacks will be determined in order to protect our parachute system against cyber attacks. Whether our proposed authentication scheme meets these requirements will be determined by a security assessment.

5.1. Anonymous Identity

The real identity of the parachute is hidden by anonymising it with mathematical methods. This is done to prevent the tracking of the parachute. For this purpose, an anonymous identity is created by hiding the identity information of the system. An anonymous identity AID_x is created using cryptography methods of the parachute's real identity ID_x . The creation of this anonymous identity is carried out by the Certificate Authority (CA) of the unit performing the operation. In this way, obtaining the real identity information from the anonymous identity information can only be performed by the CA. The real identities of systems with anonymous identities are very difficult and take a long time to reveal by attackers outside the CA [45]. In the proposed AFAPS scheme, the real identity ID_x is not transmitted directly; instead, a session-dependent anonymous identity AID_x is used during online authentication.

5.2. Identity Authentication

Identity authentication is required to verify whether the received parachute-originated message has been generated by a legitimate and mission-authorized parachute PA_x . In the proposed AFAPS scheme, authentication is provided through certificate-based public-key authorization and ECC-based signature verification. Before mission deployment, the certificate of PA_x is preloaded and validated by the target T . During online authentication, the target uses the received public key P_x to identify the corresponding certificate record and verifies the ECC-based authentication equation.

5.3. Message Integrity and Accuracy

Message integrity and accuracy are critical in autonomous parachute systems because any modification in mission-related data may lead to incorrect guidance, wrong target delivery, or operational failure. In the proposed AFAPS scheme, the authentication-related fields, timestamp, sequence number, nonce, ciphertext, and AES-GCM authentication tag are bound to the challenge value and signature verification process. In addition, AES-

GCM provides authenticated encryption for the protected mission payload. Therefore, any modification in C_x , τ_x , AD_x , or authentication-related parameters causes verification failure.

5.4. Location Confidentiality

Location confidentiality is a critical security requirement in autonomous parachute systems because the disclosure of the desired impact point may reveal sensitive mission or target information. In the proposed AFAPS framework, location confidentiality is not achieved only by hiding the identity of the parachute. Instead, the desired impact point DP_x is included in the protected mission payload

$$M_x = message_x \parallel DP_x \parallel Info_x \parallel T_x \parallel Seq_x$$

and encrypted using AES-GCM under an ECDH-derived session key. Therefore, DP_x is not transmitted in plaintext and cannot be recovered by an external adversary without the session key.

5.5. Traceability

Traceability is a security requirement so that the material or information supplied can be tracked by the CA performing the operation. The fact that the real identity of the system is known by the CA makes it traceable, and in the case where the system is under the control of hackers, it is removed from the network and disconnected from the center. The information that the supply item is taken out of the system is notified to the receiving units and security is ensured. In the proposed AFAPS scheme, traceability is supported by the certificate authority CA. Although the real identity of PA_x is hidden from external adversaries, CA can recover the real identity when accountability, incident investigation, or revocation is required.

5.6. Unlinkability

In the parachute system, the creation of anonymous identities during each message generation will provide unlinkability. In this way, hackers cannot establish a connection between anonymous identities and messages. If the anonymous identity did not change during each message transmission, it could be tracked by hackers.

5.7. Non-Repudiation

Intentional or unintentional information change will be prevented by ensuring that the recorded information of the executed operation cannot be changed later and is permanent [73]. The sender will bear the responsibility for the operations it has performed and the errors that occur will be kept accountable.

5.8. Man in the Middle Attack (MITM)

In addition to the systems guided to predetermined coordinates, for systems remote-controlled by paratroopers or ground crew exiting the aircraft with the payload, unwanted persons should be prevented from entering between the transmitter and the receiver. For this purpose, protection against MITM attacks is an important requirement in the proposed model [53].

5.9. Impersonation Attack

In the proposed AFAPS scheme, traceability is supported by the certificate authority CA. Although the real identity of PA_x is hidden from external adversaries, CA can recover the real identity when accountability, incident investigation, or revocation is required.

5.10. Replay Attack

A replay attacker may capture a previously valid authentication message and retransmit it later to deceive the target. To prevent replay attacks, each online authentication message in AFAPS includes the timestamp T_x , sequence number Seq_x , AES-GCM nonce N_x , and ephemeral message public key P_{mx} . The target accepts a message only if T_x is within the allowed time window and the tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

has not been previously accepted. Since these freshness-related values are also bound to the associated data and the challenge value, replaying or modifying an old message causes the verification process to fail.

6. The Proposed Authentication Scheme

This section presents the proposed AFAPS authentication scheme for securing autonomous ram-air parachute systems. The proposed scheme is designed to provide authentication, integrity, freshness, conditional identity privacy, traceability, and encrypted mission-payload delivery between the parachute PA_x and the target T . Unlike a purely signature-based authentication mechanism, the AFAPS scheme combines ECC-based authentication with ECDH-derived session-key establishment and AES-GCM authenticated encryption. Therefore, mission-related information, including the mission message, desired impact point, and information-replenishment payload, is not transmitted in plaintext.

The system model consists of three main entities: the certificate authority CA , the autonomous parachute PA_x , and the target T . The certificate authority is responsible for system initialization, credential generation, certificate issuance, and revocation management. The parachute PA_x represents the autonomous airdrop platform that carries the mission payload and generates the authenticated encrypted message. The target T represents the authorized receiver that verifies the parachute, checks message freshness, derives the session key, and recovers the encrypted mission payload.

The proposed AFAPS scheme consists of the following phases:

1. System setup and design-parameter definition.
2. Pre-mission provisioning and key management.
3. Anonymous identity generation.
4. Online authentication and encrypted mission-payload delivery.
5. Target-side verification and payload recovery.
6. Replay protection and revocation handling.

Parachutes can be used to carry mission information, supplies, and other critical payloads to the target. In the proposed system model, each parachute must be registered and authorized by the certificate authority CA before being deployed for a mission. The certificate authority maintains the credential information of the parachutes included in the system and is responsible for certificate issuance and revocation management.

The target T represents the authorized receiver that verifies whether the received parachute-originated message has been generated by a legitimate and mission-authorized parachute PA_x . This verification is necessary because malicious third parties may attempt to deliver false mission information, unauthorized payloads, or forged authentication messages to the target. Therefore, a cryptographic authentication and encrypted mission-payload delivery scheme is required between PA_x and T .

If a registered parachute is captured or suspected to be compromised, its certificate and public key are revoked by the certificate authority. The target rejects authentication

attempts associated with revoked or unauthorized parachute credentials. The notation and design parameters used in the proposed scheme are summarized in Table 1.

Table 1. Design parameters and notations used in the proposed AFAPS scheme.

Notation	Description
CA	Certificate authority
PA_x	x -th autonomous parachute
T	Target or authorized receiver
E	Elliptic curve over a finite field
F_p	Finite prime field
G	Additive elliptic-curve group
p, q	Large prime numbers
P	Base point of the elliptic curve
a, b	Elliptic-curve parameters
$\mathbb{Z}_q^*$	Set of non-zero integers modulo q
m	Private key of the certificate authority CA
P_{CA}	Public key of the certificate authority, $P_{CA} = m \cdot P$
sk_T	Private key of the target T
PK_T	Public key of the target, $PK_T = sk_T \cdot P$
p_x	Private key of PA_x
P_x	Public key of PA_x
$Cert_x$	Certificate of PA_x issued by CA
ID_x	Real identity of PA_x
AID_{x1}	Partial anonymous identity of PA_x
AID_x	Dynamic anonymous identity of PA_x
f_x, t_x	Fresh random values selected by PA_x
Q_x	Ephemeral ECC value, $Q_x = f_x \cdot P_{CA}$
P_{mx}	Ephemeral message public key, $P_{mx} = t_x \cdot P$
$message_x$	Mission message
DP_x	Desired impact point or target-location information
$Info_x$	Information-replenishment payload
M_x	Protected mission payload
T_x	Timestamp
Seq_x	Sequence number
N_x	AES-GCM nonce
C_x	Ciphertext of the encrypted mission payload
τ_x	AES-GCM authentication tag
AD_x	Associated data used in AES-GCM
Z_x	ECDH shared secret
K_x	Session key derived from Z_x
U_x	Challenge value generated by H_2
S_x	Signature component generated by PA_x
H_1, H_2, H_3	Secure one-way hash functions
KDF	Key derivation function
$AES-GCM$	Authenticated encryption algorithm
$\parallel$	Concatenation operation
$\oplus$	XOR operation
$Encode(\cdot)$	Encoding function for elliptic-curve values
$Bin_{\ell_q}(\cdot)$	Conversion to an ℓ_q -bit binary string

6.1. System Setup and Design-Parameter Definition

In this phase, the certificate authority CA defines the public system parameters and cryptographic primitives used in the proposed AFAPS scheme. The CA first selects an elliptic curve E over a finite prime field F_p . Let G be an additive cyclic group of prime order q , and let $P \in G$ be the base point of the elliptic curve. The curve parameters a and b are selected such that the elliptic curve satisfies the non-singularity condition

$$4a^3 + 27b^2 \neq 0 \pmod{p}.$$

The security of the ECC-based operations relies on the hardness of the elliptic-curve discrete logarithm problem. Therefore, given P and $x \cdot P$, it is computationally infeasible for an adversary to derive the scalar value x .

The CA defines three secure one-way hash functions as follows:

$$H_1 : \{0, 1\}^* \times G \rightarrow \mathbb{Z}_q^*,$$

$$H_2 : \{0, 1\}^* \times G \rightarrow \mathbb{Z}_q^*,$$

$$H_3 : G \rightarrow \mathbb{Z}_q^*.$$

Here, H_1 is used in partial anonymous identity generation, H_2 is used in challenge generation for authentication, and H_3 is used in dynamic anonymous identity generation.

In addition, the system defines an encoding function $Encode(\cdot)$ for elliptic-curve values and a binary conversion function $Bin_{\ell_q}(\cdot)$, where

$$\ell_q = \lceil \log_2 q \rceil.$$

The function $Bin_{\ell_q}(\cdot)$ converts an element of $\mathbb{Z}_q^*$ into an ℓ_q -bit binary string so that it can be used in XOR-based anonymous identity masking.

The system also defines a key derivation function KDF and the authenticated encryption algorithm $AES\text{-}GCM$. The KDF is used to derive the session key from the ECDH shared secret, while $AES\text{-}GCM$ is used to provide confidentiality and integrity for the mission payload.

The CA selects its private key

$$m \in \mathbb{Z}_q^*$$

and computes its public key as

$$P_{CA} = m \cdot P.$$

Finally, the CA publishes the public system parameters

$$\{E, F_p, G, p, q, P, P_{CA}, H_1, H_2, H_3, KDF, AES\text{-}GCM, Encode(\cdot), Bin_{\ell_q}(\cdot)\}.$$

The private key m is kept secret by the CA.

6.2. Pre-Mission Provisioning and Key Management

In this phase, the long-term credentials of the target T and the parachute PA_x are generated before mission deployment. This phase is performed in a trusted pre-mission environment.

First, the target T selects its private key

$$sk_T \in \mathbb{Z}_q^*$$

and computes its public key as

$$PK_T = sk_T \cdot P.$$

The private key sk_T is kept secret by the target, while PK_T is made available to authorized parachutes before the mission.

For each parachute PA_x , a private key

$$p_x \in \mathbb{Z}_q^*$$

is generated during trusted provisioning. The corresponding public key of PA_x is computed as

$$P_x = p_x \cdot P_{CA}.$$

The private key p_x is stored only inside PA_x , while P_x is used as the certified public key of the parachute.

The certificate authority CA issues a mission credential for PA_x as

$$Cert_x = Sig_{CA}(P_x \parallel Validity \parallel Role \parallel MissionID).$$

This certificate binds the public key P_x of PA_x to its validity information, role, and mission identifier. Before mission deployment, the target T stores and validates $Cert_x$. Therefore, $Cert_x$ is treated as a preloaded mission credential and is not transmitted in every online authentication message.

During online authentication, the target uses the received public key P_x to identify the corresponding preloaded certificate record. If the certificate is valid and PA_x is authorized for the assigned mission, the target continues the verification process. Otherwise, the message is rejected.

The private key p_x of PA_x must be stored in protected non-volatile memory or in a tamper-resistant secure element when available. The private key m of CA and the private key sk_T of the target must never be transmitted over the wireless channel.

Runtime secret values such as f_x , t_x , the ECDH shared secret Z_x , and the session key K_x are generated during the online authentication phase and must be deleted after use. In addition, each online authentication session must use fresh random values and a unique AES-GCM nonce N_x .

If a deployed parachute is physically captured or suspected to be compromised, the corresponding certificate $Cert_x$ and public key P_x must be revoked by the certificate authority. The target rejects all subsequent authentication attempts associated with revoked parachute credentials. The compromise of one parachute does not reveal the private keys of other parachutes, the private key of CA , or the private key of the target T .

6.3. Anonymous Identity Generation

This phase defines the anonymous identity generation mechanism used to protect the real identity of the parachute PA_x during online authentication. The real identity of the parachute is denoted by ID_x . This identity is not transmitted over the public wireless channel.

After the public key P_x of PA_x is generated during the pre-mission provisioning phase, the certificate authority CA computes the partial anonymous identity of PA_x as

$$AID_{x1} = ID_x \oplus Bin_{\ell_q}(H_1(Encode(m), P_x)),$$

where m is the private key of CA , P_x is the certified public key of PA_x , and $Bin_{\ell_q}(\cdot)$ converts the hash output into an ℓ_q -bit binary string.

The value AID_{x1} is securely provisioned to PA_x before mission deployment. Since AID_{x1} is generated using the private key m of CA , only the certificate authority can later recover the real identity ID_x when traceability is required.

During each online authentication session, PA_x selects a fresh random value

$$t_x \in \mathbb{Z}_q^*$$

and computes the ephemeral message public key as

$$P_{mx} = t_x \cdot P.$$

Using the same fresh value t_x , PA_x generates the dynamic anonymous identity as

$$AID_x = AID_{x1} \oplus \text{Bin}_{\ell_q}(H_3(t_x \cdot P_{CA})).$$

Since t_x is freshly selected for each online authentication session, the transmitted anonymous identity AID_x changes from one session to another. Therefore, external adversaries cannot directly obtain the real identity ID_x from the transmitted anonymous identity. In addition, the use of fresh session-dependent anonymous identities helps reduce the linkability of different authentication messages.

6.4. Online Authentication and Encrypted Mission-Payload Delivery

In this phase, the parachute PA_x generates an authenticated and encrypted online message for the target T . This phase provides authentication, freshness, integrity binding, and encrypted mission-payload delivery.

At the beginning of each online authentication session, PA_x selects fresh random values

$$f_x, t_x \leftarrow_R \mathbb{Z}_q^*.$$

The value f_x is used for ECC-based authentication, while t_x is used for dynamic anonymous identity generation and ECDH-based session-key establishment.

The parachute PA_x computes the ephemeral ECC values

$$Q_x = f_x \cdot P_{CA},$$

and

$$P_{mx} = t_x \cdot P.$$

Then, the dynamic anonymous identity is generated as

$$AID_x = AID_{x1} \oplus \text{Bin}_{\ell_q}(H_3(t_x \cdot P_{CA})).$$

To establish a session key with the target, PA_x computes the ECDH shared secret as

$$Z_x = t_x \cdot PK_T,$$

where PK_T is the public key of the target. Then, the session key is derived as

$$K_x = \text{KDF}(\text{Encode}(Z_x) \parallel AID_x \parallel T_x \parallel Seq_x \parallel P_{mx}).$$

The protected mission payload is defined as

$$M_x = \text{message}_x \parallel DP_x \parallel Info_x \parallel T_x \parallel Seq_x,$$

where message_x denotes the mission message, DP_x denotes the desired impact point, $Info_x$ denotes the information-replenishment payload, T_x denotes the timestamp, and Seq_x denotes the sequence number.

The associated data used in AES-GCM is defined as

$$AD_x = AID_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel Seq_x.$$

The associated data are not encrypted, but they are authenticated by AES-GCM and bound to the authentication process.

The parachute PA_x generates a unique AES-GCM nonce N_x for the current online authentication session. Then, the mission payload is encrypted and authenticated as

$$(C_x, \tau_x) = \text{AES-GCM.Enc}_{K_x, N_x}(M_x, AD_x),$$

where C_x is the ciphertext and τ_x is the AES-GCM authentication tag. Therefore, $message_x$, DP_x , and $Info_x$ are not transmitted in plaintext.

After generating the ciphertext and authentication tag, PA_x computes the challenge value as

$$U_x = H_2(AD_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x).$$

This challenge binds the associated data, AES-GCM nonce, ciphertext, authentication tag, and ephemeral ECC value Q_x to the signature component.

Finally, PA_x computes the signature component as

$$S_x = p_x + U_x f_x \pmod{q}.$$

The online authentication and encrypted mission-payload delivery message transmitted from PA_x to the target T is

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\}.$$

It should be noted that the certificate $Cert_x$ is not transmitted in this online message because it is preloaded and validated by the target before mission deployment.

6.5. Target-Side Verification and Payload Recovery

After receiving the online authentication and encrypted mission-payload delivery message

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\},$$

the target T verifies the authenticity, freshness, and integrity of the received message before accepting the mission payload.

First, the target uses the received public key P_x to identify the corresponding preloaded certificate record of PA_x . The target checks whether the certificate is valid for the current mission by verifying its validity information, role, and mission identifier. If no valid certificate record is found for P_x , the message is rejected.

Second, the target validates the received elliptic-curve points P_x , Q_x , and P_{mx} . This validation ensures that the received points belong to the correct elliptic-curve group and prevents invalid-curve or malformed-point attacks.

Third, the target checks the freshness of the received message. The timestamp T_x must be within the allowed time window. In addition, the tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

must not have been previously accepted. If the timestamp is expired or the tuple has already been recorded in the replay cache, the message is rejected.

The target reconstructs the associated data as

$$AD_x = AID_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel Seq_x.$$

Then, the target recomputes the challenge value as

$$U_x^* = H_2(AD_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x).$$

The ECC-based authentication equation is verified as

$$S_x \cdot P_{CA} \stackrel{?}{=} P_x + U_x^* \cdot Q_x.$$

If this equation does not hold, the message is rejected.

The correctness of the verification equation can be shown as follows. Since

$$S_x = p_x + U_x f_x \pmod{q},$$

multiplying both sides by P_{CA} gives

$$S_x \cdot P_{CA} = (p_x + U_x f_x) \cdot P_{CA}.$$

Therefore,

$$S_x \cdot P_{CA} = p_x \cdot P_{CA} + U_x f_x \cdot P_{CA}.$$

Since

$$P_x = p_x \cdot P_{CA}$$

and

$$Q_x = f_x \cdot P_{CA},$$

the equation becomes

$$S_x \cdot P_{CA} = P_x + U_x \cdot Q_x.$$

For a valid and unmodified message, the target obtains

$$U_x^* = U_x.$$

Thus, the verification equation

$$S_x \cdot P_{CA} = P_x + U_x^* \cdot Q_x$$

holds only for a valid authentication message generated by the legitimate parachute PA_x .

After successful signature verification, the target derives the ECDH shared secret using its private key sk_T and the received ephemeral public value P_{mx} :

$$Z_x = sk_T \cdot P_{mx}.$$

Since

$$P_{mx} = t_x \cdot P$$

and

$$PK_T = sk_T \cdot P,$$

the shared secret derived by the target is equivalent to the shared secret computed by the parachute:

$$sk_T \cdot P_{mx} = sk_T \cdot t_x P = t_x \cdot sk_T P = t_x \cdot PK_T.$$

The target then derives the session key as

$$K_x = KDF(Encode(Z_x) \parallel AID_x \parallel T_x \parallel Seq_x \parallel P_{mx}).$$

Using K_x , N_x , and AD_x , the target verifies the AES-GCM authentication tag τ_x and decrypts the ciphertext C_x . If AES-GCM tag verification fails, the mission payload is rejected. If the verification succeeds, the target recovers

$$M_x = message_x \parallel DP_x \parallel Info_x \parallel T_x \parallel Seq_x.$$

Finally, after successful authentication, freshness verification, and AES-GCM tag verification, the target accepts the mission payload and records the tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

in the replay cache. Runtime secret values such as Z_x and K_x are deleted after use.

6.6. Replay Protection and Revocation Handling

The proposed AFAPS scheme uses timestamp verification, sequence-number checking, nonce uniqueness, and ephemeral ECC values to prevent replay attacks. Each online authentication message includes the timestamp T_x , sequence number Seq_x , AES-GCM nonce N_x , and ephemeral message public key P_{mx} . These values are included in the associated data

$$AD_x = AID_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel Seq_x,$$

and are also bound to the challenge value

$$U_x = H_2(AD_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x).$$

When the target T receives an online authentication message, it first checks whether T_x is within the allowed time window. In the proposed AFAPS implementation, the allowed time window is denoted by ΔT . Unless a mission-specific value is defined during pre-mission configuration, ΔT is set to 60 s. The clocks of PA_x and T are assumed to be synchronized before mission deployment using the onboard real-time clock and, when available, GPS-disciplined time information. The value of ΔT is selected to cover the expected wireless communication latency, processing delay, and maximum clock drift during the authentication interval.

Accordingly, the target accepts the timestamp freshness condition only if

$$|T_{recv} - T_x| \leq \Delta T,$$

where T_{recv} denotes the local reception time of the target. A delayed but legitimate message is accepted only if it satisfies this time-window condition and the tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

has not been previously accepted. If a message arrives after the allowed time window, it is rejected even if its cryptographic verification succeeds. In such a case, a new authentication message must be generated with a fresh timestamp, sequence number, AES-GCM nonce, and ephemeral ECC value.

Then, the target checks whether the tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

has already been accepted. If this tuple is found in the replay cache, the message is considered a replayed message and is rejected.

The sequence number Seq_x is used to detect repeated or out-of-order authentication messages associated with the same parachute public key P_x . The nonce N_x must be unique for each AES-GCM encryption under the derived session key K_x . The ephemeral public value P_{mx} is generated from the fresh random value t_x and provides session freshness for both anonymous identity generation and ECDH-based session-key establishment.

If an adversary replays a previously captured message, the timestamp and replay-cache verification fail. If the adversary modifies any of the freshness-related fields, the recomputed challenge value U_x^* changes, and the ECC-based authentication equation fails. In addition, any modification in the ciphertext C_x , authentication tag τ_x , or associated data AD_x causes AES-GCM tag verification to fail.

Revocation is handled by the certificate authority CA . If a registered parachute PA_x is physically captured, suspected to be compromised, or no longer authorized for a mission, the corresponding certificate $Cert_x$ and public key P_x are revoked. Since the certificate is preloaded before mission deployment, the target T should be provisioned with the current list of authorized and revoked parachute credentials. During online authentication, if the received public key P_x corresponds to a revoked or unauthorized credential, the target rejects the message.

The compromise of one parachute does not reveal the private keys of other parachutes, the private key m of the certificate authority, or the private key sk_T of the target. In addition, runtime secrets such as f_x , t_x , Z_x , and K_x are not stored persistently and are deleted after use. Therefore, AFAPS provides replay protection, certificate-based revocation, and post-compromise containment.

7. Security Evaluation

This section evaluates the security of the proposed AFAPS protocol from both informal and formal perspectives. First, the adversary model is defined by specifying the capabilities of an attacker in the wireless communication environment of the autonomous ram-air parachute system. Then, the main security properties of AFAPS are analyzed in detail, including identity confidentiality, authentication, message integrity, location confidentiality, traceability, unlinkability, non-repudiation, MITM resistance, and impersonation resistance. Finally, a formal security analysis based on BAN Logic is provided to validate the authentication, freshness, and mission-payload acceptance properties of the proposed protocol.

7.1. Adversary Model

The proposed AFAPS protocol is analyzed under a public-channel adversary model. The communication between the parachute PA_x and the target is assumed to take place over a wireless and potentially insecure channel. Therefore, an adversary $\mathcal{A}$ may eavesdrop on all transmitted messages, replay previously captured messages, modify message components, delete messages, inject forged messages, and attempt man-in-the-middle or impersonation attacks.

During the online authentication phase, the message transmitted from PA_x to the target is

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\}.$$

The certificate of PA_x is assumed to be preloaded and validated before mission deployment. Therefore, $Cert_x$ is treated as a mission credential stored by the target and is not transmitted in every online authentication message. The target uses the received public key P_x to identify the corresponding preloaded certificate record and to check whether PA_x is authorized for the assigned mission.

The adversary $\mathcal{A}$ is assumed to know all public parameters of the system, including the elliptic curve parameters, base point P , public key of the certificate authority P_{CA} , public

key of the target PK_T , public hash functions, KDF specification, and AES-GCM algorithm. However, $\mathcal{A}$ cannot obtain the private key m of the certificate authority or the private key sk_T of the legitimate target. In addition, before physical capture, the private key p_x of the legitimate parachute PA_x is assumed to be protected inside the device.

The adversary may capture a deployed parachute after landing and attempt to extract stored credentials from the device. In such a case, the corresponding certificate and public key of the captured parachute must be revoked by the certificate authority. The compromise of one parachute is not assumed to reveal the private keys of other parachutes, the certificate authority private key, or the target private key. Therefore, physical capture is handled through key isolation, certificate revocation, and post-compromise containment.

The adversary may also attempt replay attacks by retransmitting previously accepted messages. To resist such attacks, the target checks the timestamp T_x , sequence number Seq_x , nonce N_x , and ephemeral public value P_{mx} . A received message is accepted only if its timestamp is within the allowed time window and the freshness tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

has not been previously accepted.

All received elliptic-curve points, including P_x , Q_x , and P_{mx} , are validated before being used in cryptographic computations. This prevents invalid-curve and malformed-point attacks. In addition, the protocol assumes that cryptographic primitives such as the hash functions, KDF, ECDH operation, and AES-GCM are implemented securely.

Finally, cyber-physical attacks such as GPS spoofing, RF jamming, trajectory manipulation, and abnormal flight behavior are considered important threats for autonomous parachute systems. However, these attacks cannot be completely mitigated by cryptographic authentication alone. Therefore, the proposed cryptographic framework focuses on communication security, while the 6-DOF dynamics model provides a physical basis for future trajectory-consistency verification and kinematic anomaly detection mechanisms.

7.2. Informal Security Analysis

This subsection provides an informal security analysis of the proposed AFAPS protocol under the adversary model defined in Section 7.1. The analysis discusses the main security properties of AFAPS, including identity confidentiality, authentication, message integrity, location confidentiality, traceability, unlinkability, non-repudiation, MITM resistance, and impersonation resistance [74,75].

7.2.1. Identity Confidentiality

In the proposed AFAPS protocol, the real identity ID_x of the parachute PA_x is not transmitted over the public wireless channel. Instead, a dynamic anonymous identity AID_x is used in the online authentication message. The initial anonymous identity is generated as

$$AID_{x1} = ID_x \oplus \text{Bin}_{\ell_q}(H_1(\text{Encode}(m), P_x)),$$

where m is the private key of the certificate authority, P_x is the public key of PA_x , and $\text{Bin}_{\ell_q}(\cdot)$ converts the hash output into an ℓ_q -bit string.

During each online authentication session, PA_x selects a fresh random value $t_x \in \mathbb{Z}_q^*$ and computes

$$P_{mx} = t_x \cdot P.$$

The transmitted anonymous identity is then computed as

$$AID_x = AID_{x1} \oplus \text{Bin}_{\ell_q}(H_3(t_x \cdot P_{CA})).$$

Since the adversary does not know the certificate authority private key m and cannot derive t_x from $P_{mx} = t_x P$ under the elliptic-curve discrete logarithm assumption, the real identity ID_x cannot be recovered from AID_x . Therefore, AFAPS provides identity confidentiality against passive eavesdroppers.

7.2.2. Authentication

Authentication in AFAPS is achieved through certificate-based public-key authorization and ECC-based signature verification. Before mission deployment, the certificate

$$Cert_x = Sig_{CA}(P_x \parallel Validity \parallel Role \parallel MissionID)$$

is preloaded and validated by the target. Therefore, the certificate is not transmitted in each online authentication message. During online authentication, the target uses the received P_x value to identify the corresponding preloaded certificate record and to verify whether PA_x is authorized for the assigned mission.

For online message authentication, PA_x selects a fresh random value $f_x \in \mathbb{Z}_q^*$ and computes

$$Q_x = f_x \cdot P_{CA}.$$

Then, the challenge value is computed as

$$U_x = H_2(AD_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x),$$

where

$$AD_x = AID_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel Seq_x.$$

The signature component is generated as

$$S_x = p_x + U_x f_x \pmod{q}.$$

After receiving the message, the target recomputes the challenge value U_x^* and verifies

$$S_x \cdot P_{CA} \stackrel{?}{=} P_x + U_x^* \cdot Q_x.$$

Since

$$S_x \cdot P_{CA} = (p_x + U_x f_x) \cdot P_{CA},$$

and

$$P_x = p_x \cdot P_{CA}, \quad Q_x = f_x \cdot P_{CA},$$

the verification equation holds only if the message was generated using the legitimate private key p_x and the fresh random value f_x . Therefore, an adversary cannot generate a valid authentication message without knowing the private key of PA_x .

7.2.3. Message Integrity

AFAPS provides message integrity through the combined use of ECC-based authentication and AES-GCM authentication. The challenge value

$$U_x = H_2(AD_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x)$$

binds the associated data, nonce, ciphertext, authentication tag, and ephemeral ECC value Q_x to the signature component S_x . Therefore, any modification in AID_x , P_x , Q_x , P_{mx} , T_x , Seq_x , N_x , C_x , or τ_x changes the recomputed challenge value U_x^* at the target side and causes the ECC verification equation to fail.

In addition, the encrypted mission payload is protected by AES-GCM. The parachute computes

$$(C_x, \tau_x) = \text{AES-GCM.Enc}_{K_x, N_x}(M_x, AD_x),$$

where C_x is the ciphertext and τ_x is the authentication tag. If an adversary modifies either the ciphertext or the associated data, AES-GCM tag verification fails at the target side. Therefore, AFAPS ensures the integrity of both authentication-related fields and encrypted mission-payload data.

7.2.4. Location Confidentiality

The proposed AFAPS protocol protects mission-related and target-location information by encrypting the mission payload using an ECDH-derived session key. As defined in Section 6.4, the protected mission payload M_x includes the desired impact point and other mission-related information.

The parachute computes the ECDH shared secret as

$$Z_x = t_x \cdot PK_T,$$

where PK_T is the public key of the target. The target computes the same shared secret as

$$Z_x = sk_T \cdot P_{mx},$$

where

$$P_{mx} = t_x \cdot P.$$

Since

$$t_x \cdot PK_T = t_x \cdot sk_T \cdot P = sk_T \cdot t_x \cdot P = sk_T \cdot P_{mx},$$

both parties derive the same shared secret.

The session key is derived as

$$K_x = \text{KDF}(\text{Encode}(Z_x) \parallel \text{AID}_x \parallel T_x \parallel \text{Seq}_x \parallel P_{mx}).$$

The mission payload is then encrypted and authenticated using AES-GCM. Since the adversary does not know t_x or sk_T , the shared secret Z_x and the session key K_x cannot be derived. Therefore, the desired impact point and other mission-related information remain confidential against passive and active attackers.

7.2.5. Traceability

Although the real identity of PA_x is hidden from public observers, the certificate authority can recover the real identity when traceability is required. Since the certificate authority knows its private key m , it can compute

$$m \cdot P_{mx} = m \cdot t_x P = t_x \cdot mP = t_x \cdot P_{CA}.$$

Then, the certificate authority can recover AID_{x1} as

$$\text{AID}_{x1} = \text{AID}_x \oplus \text{Bin}_{\ell_q}(H_3(m \cdot P_{mx})).$$

Finally, the real identity can be obtained as

$$\text{ID}_x = \text{AID}_{x1} \oplus \text{Bin}_{\ell_q}(H_1(\text{Encode}(m), P_x)).$$

Therefore, AFAPS provides conditional identity privacy: external adversaries cannot reveal the real identity of PA_x , while the trusted certificate authority can trace the identity when required for accountability, incident investigation, or mission auditing.

7.2.6. Unlinkability

AFAPS uses fresh session-dependent values to reduce linkability between different authentication sessions. In each online authentication session, the parachute selects fresh random values f_x and t_x , which generate new values

$$Q_x = f_x \cdot P_{CA}$$

and

$$P_{mx} = t_x \cdot P.$$

Moreover, the transmitted anonymous identity AID_x changes with t_x , since it includes the masking value

$$H_3(t_x \cdot P_{CA}).$$

Therefore, an external adversary cannot link two sessions using AID_x , Q_x , or P_{mx} if fresh random values are properly generated.

However, if the same long-term public key P_x is repeatedly transmitted across multiple missions, an external observer may correlate messages belonging to the same public key. Therefore, strong session unlinkability requires the use of mission-specific or short-term certified public keys. Under this deployment setting, AFAPS provides unlinkability by ensuring that the visible authentication values change across sessions and missions.

7.2.7. Non-Repudiation

AFAPS provides operational non-repudiation through certificate-bound ECC authentication. The public key P_x of the parachute is certified by the certificate authority before mission deployment, and the online authentication message is validated through the ECC verification equation

$$S_x \cdot P_{CA} \stackrel{?}{=} P_x + U_x^* \cdot Q_x.$$

Since a valid signature component S_x can only be generated using the private key p_x corresponding to the certified public key P_x , an accepted authentication message can be attributed to the corresponding certified parachute.

This property provides operational accountability in the trusted-authority model. If the private key p_x is generated and stored only inside PA_x , the accepted message provides strong evidence that the message originated from the corresponding parachute. If the certificate authority or mission authority participates in key generation or key storage, the property should be interpreted as operational accountability rather than absolute legal non-repudiation.

7.2.8. MITM Resistance

AFAPS resists man-in-the-middle attacks by binding the authentication values, encrypted payload, timestamp, sequence number, nonce, and ephemeral ECDH value into the signature verification process. An adversary attempting to intercept and modify the message must produce a valid tuple

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\}$$

that satisfies the ECC verification equation and the AES-GCM tag verification. Without knowing the private key p_x , the adversary cannot generate a valid S_x . Without knowing

t_x or sk_T , the adversary cannot derive the session key K_x required to generate a valid ciphertext and authentication tag.

Furthermore, the ECDH value P_{mx} is included in both the associated data and the KDF input:

$$K_x = \text{KDF}(\text{Encode}(Z_x) \parallel \text{AID}_x \parallel T_x \parallel \text{Seq}_x \parallel P_{mx}).$$

Thus, replacing P_{mx} changes both the associated data and the derived session key, causing verification failure. Therefore, AFAPS prevents an adversary from successfully modifying, replacing, or relaying authentication messages as a valid man-in-the-middle.

7.2.9. Impersonation Resistance

An adversary may attempt to impersonate a legitimate parachute by generating a forged authentication message. However, successful impersonation requires both a valid preloaded certificate record associated with P_x and a valid ECC authentication component S_x . Since the adversary does not know the private key p_x , it cannot compute

$$S_x = p_x + U_x f_x \pmod{q}$$

for a valid challenge value U_x .

The adversary may also attempt to reuse an old valid message. However, the target checks the timestamp T_x , sequence number Seq_x , nonce N_x , and ephemeral public value P_{mx} . If the same freshness tuple has already been accepted or the timestamp is outside the allowed time window, the message is rejected. Therefore, AFAPS resists both direct impersonation and replay-based impersonation attacks.

7.2.10. Replay Attack Resistance

The proposed AFAPS protocol resists replay attacks through the combined use of timestamp verification, sequence-number checking, AES-GCM nonce uniqueness, ephemeral ECC values, and replay-cache control. Each online authentication message includes the freshness-related values T_x , Seq_x , N_x , and P_{mx} . These values are included in the associated data

$$\text{AD}_x = \text{AID}_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel \text{Seq}_x,$$

and are also bound to the challenge value

$$U_x = H_2(\text{AD}_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x).$$

The timestamp verification is performed using the operational time-window parameter ΔT . Unless a mission-specific value is configured before deployment, ΔT is set to 60 s. The target accepts the timestamp freshness condition only if

$$|T_{\text{recv}} - T_x| \leq \Delta T,$$

where T_{recv} denotes the local reception time of the target. Therefore, a delayed but legitimate message is accepted only if it remains within this time window and its freshness tuple has not been previously accepted.

Assume that an adversary $\mathcal{A}$ captures a valid online authentication message

$$\mathcal{M}_x = \{\text{AID}_x, P_x, Q_x, P_{mx}, T_x, \text{Seq}_x, N_x, C_x, \tau_x, S_x\}$$

and retransmits the same message to the target T . If $\mathcal{A}$ replays the message without modification, the replayed message contains the same freshness tuple

$$(P_x, Seq_x, N_x, P_{mx}).$$

Since this tuple is recorded in the replay cache after the first successful acceptance, the target detects that the same tuple has already been accepted and rejects the replayed message. If the replayed message is received outside the allowed time window, it is also rejected because the timestamp T_x is no longer valid.

If $\mathcal{A}$ modifies one or more freshness-related fields, such as T_x , Seq_x , N_x , or P_{mx} , in order to bypass replay-cache verification, the recomputed challenge value U_x^* changes at the target side. Since the signature component S_x was generated for the original challenge value U_x , the verification equation

$$S_x \cdot P_{CA} \stackrel{?}{=} P_x + U_x^* \cdot Q_x$$

does not hold for the modified message.

Moreover, if $\mathcal{A}$ attempts to generate a new valid signature component for the modified message, it must compute

$$S'_x = p_x + U_x^* f_x \pmod{q}.$$

However, this requires the private key p_x of the legitimate parachute PA_x , which is computationally infeasible for the adversary under the elliptic-curve discrete logarithm assumption.

In addition, if $\mathcal{A}$ modifies the ciphertext C_x , authentication tag τ_x , nonce N_x , or associated data AD_x , the AES-GCM tag verification fails. If $\mathcal{A}$ attempts to generate a new valid ciphertext and tag, it must derive the session key

$$K_x = \text{KDF}(\text{Encode}(Z_x) \parallel \text{AID}_x \parallel T_x \parallel Seq_x \parallel P_{mx}),$$

which requires the ECDH shared secret Z_x . Since $\mathcal{A}$ does not know either the fresh secret t_x of PA_x or the private key sk_T of the target, it cannot derive K_x .

Therefore, an old valid message cannot be successfully reused either in its original form or in a modified form. Thus, the proposed AFAPS protocol resists replay attacks.

7.3. Formal Security Analysis Using BAN Logic

This subsection presents a formal security analysis of the proposed AFAPS protocol using BAN Logic. The purpose of this analysis is to validate the main authentication-related security goals of the protocol, namely target-side authentication of the parachute PA_x , freshness of the received online authentication message, and acceptance of the encrypted mission payload by the target T . Since AFAPS is a one-way parachute-to-target authentication and encrypted mission-payload delivery protocol, the BAN Logic analysis focuses on the beliefs established by the target after receiving and verifying the online authentication message [61,76,77].

7.3.1. BAN Logic Notation

The BAN Logic notation used in the formal security analysis is summarized in Table 2. In this analysis, PA_x denotes the parachute, T denotes the target, and CA denotes the certificate authority. Since the symbol P is used as the elliptic-curve base point in the proposed protocol, the symbol A is used only as a generic principal in the BAN Logic notation definitions.

Table 2. BAN Logic notation used in the formal security analysis.

Notation	Meaning
$A \models X$	Principal A believes statement X .
$A \triangleleft X$	Principal A sees or receives message X .
$A \sim X$	Principal A once said message X .
$A \models\Rightarrow X$	Principal A has jurisdiction over statement X .
$\#(X)$	Statement X is fresh.
$\xrightarrow{K} A$	K is the public key of principal A .
$\{X\}_K$	Message X is protected using key K .
$\langle X \rangle_{p_x}$	Message X is authenticated using the private key p_x of PA_x .

7.3.2. Idealized Protocol Messages

In the proposed AFAPS protocol, the certificate of the parachute PA_x is preloaded and validated by the target T before mission deployment. Therefore, the certificate-related process is idealized as an offline mission-credential distribution step:

$$M_0 : CA \rightarrow T : \langle P_x, PA_x, Validity, MissionID \rangle_{SK_{CA}}.$$

This idealized message means that the certificate authority CA certifies the binding between the parachute PA_x , its public key P_x , the certificate validity information, and the mission identifier.

During the online authentication phase, PA_x sends the following message to the target:

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\}.$$

In BAN Logic form, the online authentication and encrypted mission-payload delivery message is idealized as

$$M_1 : PA_x \rightarrow T : \langle X_x \rangle_{p_x}, \{M_x\}_{K_x}.$$

Here, X_x denotes the authenticated online message context:

$$X_x = AD_x \parallel N_x \parallel C_x \parallel \tau_x,$$

where the associated data are defined as

$$AD_x = AID_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel Seq_x.$$

The protected mission payload is defined as

$$M_x = message_x \parallel DP_x \parallel Info_x \parallel T_x \parallel Seq_x.$$

The ciphertext is represented as

$$C_x = \{M_x\}_{K_x}.$$

The session key is derived from the ECDH shared secret:

$$K_x = KDF(Encode(Z_x) \parallel AID_x \parallel T_x \parallel Seq_x \parallel P_{mx}),$$

where

$$Z_x = t_x \cdot PK_T = sk_T \cdot P_{mx}.$$

7.3.3. Security Goals

The BAN Logic analysis aims to establish the following security goals at the target side.

The first goal is that the target T believes that P_x is the certified public key of the parachute PA_x :

$$G_1 : T \models \xrightarrow{P_x} PA_x.$$

The second goal is that the target T believes that PA_x once said the authenticated online message context X_x :

$$G_2 : T \models PA_x \mid \sim X_x.$$

The third goal is that the target T believes that X_x is fresh:

$$G_3 : T \models \#(X_x).$$

The fourth goal is that the target T believes that PA_x currently believes X_x :

$$G_4 : T \models PA_x \models X_x.$$

The fifth goal is that the target T accepts X_x as a valid authenticated online message:

$$G_5 : T \models X_x.$$

The sixth goal is that, after successful AES-GCM verification, the target T believes that the encrypted mission payload M_x is bound to the authenticated message generated by PA_x :

$$G_6 : T \models PA_x \models M_x.$$

The final goal is that the target T accepts the decrypted mission payload M_x :

$$G_7 : T \models M_x.$$

7.3.4. Initial Assumptions

The following assumptions are used in the BAN Logic analysis.

The target T believes that P_{CA} is the public key of the certificate authority CA :

$$A_1 : T \models \xrightarrow{P_{CA}} CA.$$

The target T believes that CA has jurisdiction over the binding between PA_x and its certified public key P_x :

$$A_2 : T \models CA \mid \Rightarrow (\xrightarrow{P_x} PA_x).$$

The target T believes that the mission credential, including its validity information and mission identifier, is fresh for the current mission:

$$A_3 : T \models \#(Validity, MissionID).$$

The target T believes that the freshness values in the online authentication message are fresh if they satisfy timestamp verification, sequence-number verification, nonce verification, and replay-cache verification:

$$A_4 : T \models \#(T_x, Seq_x, N_x, P_{mx}).$$

The target T believes that PA_x has jurisdiction over its authenticated online message context X_x :

$$A_5 : T \models PA_x \mid \Rightarrow X_x.$$

The target T believes that PA_x has jurisdiction over its own mission payload M_x :

$$A_6 : T \models PA_x \mid \Rightarrow M_x.$$

The target T believes that a valid AES-GCM tag over C_x and AD_x under the derived session key K_x proves the integrity and authenticity of the encrypted payload:

$$A_7 : T \models \text{ValidTag}(C_x, \tau_x, AD_x, K_x).$$

7.3.5. BAN Logic Rules

The following BAN Logic rules are applied in the analysis.

The message-meaning rule for public-key authentication is given as

$$\frac{T \models \xrightarrow{P_x} PA_x, \quad T \triangleleft \langle X_x \rangle_{p_x}}{T \models PA_x \mid \sim X_x}.$$

The freshness rule is given as

$$\frac{T \models \#(T_x, Seq_x, N_x, P_{mx})}{T \models \#(X_x)}.$$

The nonce-verification rule is given as

$$\frac{T \models \#(X_x), \quad T \models PA_x \mid \sim X_x}{T \models PA_x \mid \equiv X_x}.$$

The jurisdiction rule for the authenticated online message context is given as

$$\frac{T \models PA_x \mid \Rightarrow X_x, \quad T \models PA_x \mid \equiv X_x}{T \models X_x}.$$

The payload-belief rule is given as

$$\frac{T \models X_x, \quad T \models \text{ValidTag}(C_x, \tau_x, AD_x, K_x), \quad T \models PA_x \mid \Rightarrow M_x}{T \models PA_x \mid \equiv M_x}.$$

The payload-acceptance rule is given as

$$\frac{T \models PA_x \mid \equiv M_x, \quad T \models PA_x \mid \Rightarrow M_x}{T \models M_x}.$$

7.3.6. BAN Logic Proof

First, the target T receives and validates the preloaded mission credential

$$M_0 : CA \rightarrow T : \langle P_x, PA_x, \text{Validity}, \text{MissionID} \rangle_{SK_{CA}}.$$

Using assumption A_1 , the target believes that P_{CA} is the public key of the certificate authority CA :

$$T \models \xrightarrow{P_{CA}} CA.$$

After successful verification of the mission credential signed by CA, the target concludes that CA once stated the binding between P_x and PA_x :

$$T \models CA \mid \sim (\xrightarrow{P_x} PA_x).$$

Since the mission credential is fresh for the current mission according to assumption A_3 , the target obtains

$$T \models CA \models (\xrightarrow{P_x} PA_x).$$

Using the jurisdiction assumption A_2 , the target concludes

$$T \models \xrightarrow{P_x} PA_x.$$

Thus, goal G_1 is achieved.

Second, the target receives the online authentication and encrypted mission-payload delivery message

$$M_1 : PA_x \rightarrow T : \langle X_x \rangle_{p_x}, \{M_x\}_{K_x}.$$

In the actual protocol, this message corresponds to the received tuple

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\}.$$

The target recomputes the challenge value as

$$U_x^* = H_2(AD_x \parallel N_x \parallel C_x \parallel \tau_x, Q_x),$$

where

$$AD_x = AID_x \parallel P_x \parallel Q_x \parallel P_{mx} \parallel T_x \parallel Seq_x.$$

Then, the target verifies the ECC authentication equation

$$S_x \cdot P_{CA} \stackrel{?}{=} P_x + U_x^* \cdot Q_x.$$

Successful verification means that the received message is authenticated under the private key corresponding to the certified public key P_x . Therefore, the target sees the authenticated message context:

$$T \triangleleft \langle X_x \rangle_{p_x}.$$

Using G_1 and the message-meaning rule, the target concludes

$$T \models PA_x \mid \sim X_x.$$

Thus, goal G_2 is achieved.

Third, the target verifies the freshness values T_x , Seq_x , N_x , and P_{mx} . If T_x is within the allowed time window and the tuple

$$(P_x, Seq_x, N_x, P_{mx})$$

has not been previously accepted, then assumption A_4 gives

$$T \models \#(T_x, Seq_x, N_x, P_{mx}).$$

Since these freshness values are included in X_x , the freshness rule gives

$$T \models \#(X_x).$$

Thus, goal G_3 is achieved.

Fourth, from

$$T \models PA_x \mid \sim X_x$$

and

$$T \models \#(X_x),$$

the nonce-verification rule gives

$$T \models PA_x \models X_x.$$

Thus, goal G_4 is achieved.

Fifth, using assumption A_5 ,

$$T \models PA_x \Rightarrow X_x,$$

and the result

$$T \models PA_x \models X_x,$$

the jurisdiction rule gives

$$T \models X_x.$$

Thus, goal G_5 is achieved.

Sixth, the target computes the ECDH shared secret as

$$Z_x = sk_T \cdot P_{mx},$$

and derives the session key as

$$K_x = KDF(Encode(Z_x) \parallel AID_x \parallel T_x \parallel Seq_x \parallel P_{mx}).$$

Then, the target verifies the AES-GCM authentication tag τ_x over the ciphertext C_x and the associated data AD_x . If the tag verification succeeds, assumption A_7 gives

$$T \models ValidTag(C_x, \tau_x, AD_x, K_x).$$

Since the authenticated online message context X_x has already been accepted and the encrypted payload is verified under the session key derived from the authenticated value P_{mx} , the payload-belief rule gives

$$T \models PA_x \models M_x.$$

Thus, goal G_6 is achieved.

Finally, using assumption A_6 ,

$$T \models PA_x \Rightarrow M_x,$$

and the result

$$T \models PA_x \models M_x,$$

the payload-acceptance rule gives

$$T \models M_x.$$

Thus, goal G_7 is achieved.

Therefore, the BAN Logic analysis shows that the proposed AFAPS protocol enables the target T to authenticate the parachute PA_x , verify the freshness of the received on-

line authentication message, and accept the encrypted mission payload after successful cryptographic verification.

7.4. Discussion on Cyber-Physical Threats

The proposed AFAPS protocol primarily addresses communication security requirements, including authentication, integrity, freshness, identity confidentiality, traceability, and encrypted mission-payload confidentiality. However, autonomous ram-air parachute systems are cyber-physical platforms, and therefore they may also be exposed to physical-layer and navigation-layer threats.

GPS spoofing, RF jamming, trajectory manipulation, and abnormal flight behavior are important threats in autonomous aerial systems. These attacks may affect the navigation, guidance, and control behavior of the parachute even if the communication protocol itself remains cryptographically secure. Therefore, such attacks cannot be completely mitigated by authentication and encryption alone.

In the proposed framework, the 6-DOF dynamics model defines the physical operating context of the autonomous parachute system. Although the 6-DOF model is not directly used as a cryptographic primitive, it identifies the flight-state and mission-related information that must be protected during communication. In addition, it can support future trajectory-consistency verification and kinematic anomaly detection mechanisms. For example, received mission updates or navigation-related information may be checked against physically plausible position, velocity, attitude, and angular-rate transitions.

Therefore, AFAPS should be considered as the communication-security layer of a broader cyber-physical protection framework. The cryptographic protocol protects mission-related messages and target-location data, while physical-state verification mechanisms based on the 6-DOF model can complement the protocol against navigation-layer and trajectory-level attacks.

8. Performance Analysis

This section evaluates the performance of the proposed AFAPS protocol in terms of computational cost and communication overhead. Since autonomous ram-air parachute systems operate as resource-constrained airborne cyber-physical platforms, the proposed authentication framework should not only satisfy the required security properties but also remain efficient in terms of cryptographic operation count and transmitted message size. Therefore, the performance evaluation is conducted by considering the dominant cryptographic operations, the execution time of primitive operations, and the total communication overhead of the transmitted authentication and encrypted mission-payload message.

For a fair comparison, the proposed AFAPS protocol is compared with five representative authentication schemes from the UAV, IoD, and autonomous aerial communication literature: Kirsal Ever [20], Nyangaresi et al. [28], Choe and Kang [29], Shariq et al. [30] and Chen et al. [78]. These schemes were selected because they address authentication, privacy, and secure communication requirements in UAV, IoD, drone-to-drone, or airborne communication scenarios and employ comparable cryptographic mechanisms, such as ECC, bilinear pairing, digital signatures, symmetric encryption, hash functions, and privacy-preserving authentication.

The performance analysis is organized as follows. First, the average execution times of the cryptographic operations used in the evaluation are presented. Then, the computational cost of the proposed AFAPS protocol is derived according to the operations performed by the parachute PA_x and the target. Finally, the communication overhead of AFAPS is analyzed and compared with the selected schemes from the literature.

To obtain reference execution times for the cryptographic primitives, benchmark measurements were performed in a controlled software environment. The benchmark platform was a computer running Ubuntu 16.04 operating system and equipped with an Intel Core i7-7500U CPU and 8 GB RAM. The cryptographic operations were implemented in the C++ programming language using the PBC (Pairing-Based Cryptography) version 1.0.0 [79] and GMP (GNU Multiple Precision Arithmetic) version 6.3.0 [80] libraries. Each cryptographic primitive was executed 5000 times, and the average execution time was recorded in milliseconds. The resulting benchmark values are summarized in Table 3.

It should be noted that the benchmark measurements in Table 3 were not obtained directly from an ESP32 device. Therefore, these values are used as operation-level reference measurements rather than direct ESP32 execution times. This distinction is important because the absolute execution time on ESP32-class hardware depends on the selected elliptic curve, cryptographic library, compiler optimization level, clock frequency, memory configuration, and hardware-acceleration support. Nevertheless, the proposed AFAPS protocol is suitable for ESP32-class embedded implementation because ESP-IDF supports C/C++ application development and provides cryptographic functionality through Mbed TLS, including elliptic-curve-based operations, hashing, random number generation, and symmetric cryptographic primitives. Therefore, instead of claiming an unverified ESP32-specific runtime, this study evaluates the proposed protocol using dominant operation counts and benchmark-based primitive execution times.

Table 3. Average running time of cryptographic operations used in the performance analysis.

Operation	Running Time (ms)	Description
T_{BP}	4.591	Bilinear pairing operation
T_{SM}^{BP}	1.390	Scalar multiplication over bilinear pairing group
T_{PA}^{BP}	0.007	Point addition over bilinear pairing group
T_{SM}	0.3611	ECC scalar multiplication
T_{PA}	0.0029	ECC point addition
T_H	0.00017	One-way hash operation
T_{Enc}	0.0059	Symmetric encryption/decryption operation
$T_{AES-GCM}$	0.00031	AES-GCM encryption and authentication operation
T_{KDF}	0.0037	Key derivation function operation
T_{Sig}	0.0041	Digital signature operation
T_R	0.0007	Random number generation operation

8.1. Computational Cost Analysis

This subsection analyzes the computational cost of the proposed AFAPS protocol and compares it with representative UAV/IoD authentication schemes. The comparison is based on the number of dominant cryptographic operations required during the main authentication and secure communication phase of each scheme.

In the proposed AFAPS protocol, the parachute PA_x first selects two fresh random values

$$f_x, t_x \leftarrow_R \mathbb{Z}_q^*$$

and generates the nonce N_x for AES-GCM. Therefore, three random number generation operations are required on the PA_x side.

The parachute PA_x then computes the ECC-based values

$$Q_x = f_x \cdot P_{CA},$$

$$P_{mx} = t_x \cdot P,$$

$$t_x \cdot P_{CA},$$

and

$$Z_x = t_x \cdot PK_T.$$

Thus, four ECC scalar multiplications are required on the PA_x side.

The parachute PA_x also computes the anonymous-identity masking value and the challenge value. Therefore, two hash operations are required. In addition, one KDF operation is used to derive the session key, and one AES-GCM encryption/authentication operation is used to protect the encrypted mission payload. Accordingly, the computational cost on the PA_x side is expressed as

$$T_{PA_x}^{AFAPS} = 4T_{SM} + 2T_H + T_{KDF} + T_{AES-GCM} + 3T_R.$$

On the target side, the target verifies the ECC-based authentication equation and derives the ECDH shared secret. The target computes

$$S_x \cdot P_{CA},$$

$$U_x^* \cdot Q_x,$$

and

$$sk_T \cdot P_{mx}.$$

Therefore, three ECC scalar multiplications are required on the target side. In addition, the verification equation requires one ECC point addition. The target also performs one hash operation to recompute the challenge value, one KDF operation to derive the session key, and one AES-GCM decryption/tag verification operation to verify and decrypt the mission payload. Hence, the computational cost on the target side is expressed as

$$T_T^{AFAPS} = 3T_{SM} + T_{PA} + T_H + T_{KDF} + T_{AES-GCM}.$$

Accordingly, the total computational cost of the proposed AFAPS protocol is

$$T_{AFAPS} = T_{PA_x}^{AFAPS} + T_T^{AFAPS}.$$

Thus,

$$T_{AFAPS} = 7T_{SM} + T_{PA} + 3T_H + 2T_{KDF} + 2T_{AES-GCM} + 3T_R.$$

Using the benchmark values in Table 3, the total execution time of AFAPS is calculated as

$$T_{AFAPS} = 7(0.3611) + 0.0029 + 3(0.00017) + 2(0.0037) + 2(0.00031) + 3(0.0007).$$

Therefore,

$$T_{AFAPS} = 2.54123 \text{ ms.}$$

Thus, the proposed AFAPS protocol requires approximately

$$2.541 \text{ ms}$$

for one complete authentication and encrypted mission-payload delivery process under the benchmark setting.

The computational costs of the compared schemes are summarized in Table 4. To provide a consistent evaluation, the operation symbols are normalized as follows: T_{BP} denotes a bilinear pairing operation, T_{SM}^{BP} denotes a scalar multiplication over a bilinear-pairing group, T_{SM} denotes an ECC scalar multiplication, T_{PA} denotes an ECC point addition, T_H denotes a hash operation, T_{Enc} denotes symmetric encryption/decryption, T_{Sig} denotes a digital signature operation, T_{KDF} denotes a key derivation function, $T_{AES-GCM}$ denotes AES-GCM encryption/authentication, and T_R denotes random number generation.

Table 4. Computational cost comparison of AFAPS with related UAV/IoD authentication schemes.

Scheme	Scenario	Computation Cost	Time (ms)
[20]	UAV/mobile-sink authentication	$4T_{SM}^{BP} + 6T_{BP} + 17T_H$	33.1089
[28]	IoD drone-ground station authentication	$10T_{SM} + 9T_H$	3.6125
[29]	Military IoD soldier-drone authentication	$10T_{SM} + 4T_{PA} + 6T_H + 2T_R$	3.6250
[30]	Drone-to-drone authentication	$10T_{SM} + 6T_{PA} + 8T_H$	3.6298
[78]	UAV communication control	$10T_{SM} + 8T_H + 8T_{Enc} + 6T_{Sig}$	3.6842
AFAPS	Autonomous parachute mission-payload delivery	$7T_{SM} + T_{PA} + 3T_H + 2T_{KDF} + 2T_{AES-GCM} + 3T_R$	2.5412

As shown in Table 4, the proposed AFAPS protocol has the lowest computational cost among the compared schemes under the same benchmark setting. The main reason is that AFAPS avoids bilinear pairing operations and reduces the number of dominant ECC scalar multiplications to seven. In contrast, Kirsal Ever's scheme relies on bilinear pairing operations, which significantly increases the total execution time. Chen et al., Choe and Kang, Nyangaresi et al., and Shariq et al. require ten ECC scalar multiplications or additional signature, encryption, or point-addition operations in their main authentication phases.

Although AFAPS additionally performs KDF and AES-GCM operations to provide encrypted mission-payload and target-location confidentiality, these operations introduce only a small computational overhead compared with ECC scalar multiplication. Therefore, the proposed protocol achieves a favorable balance between security functionality and computational efficiency.

8.2. Communication Cost Analysis

This subsection analyzes the communication overhead of the proposed AFAPS protocol and compares it with the selected UAV/IoD authentication schemes. Communication cost is an important performance metric for autonomous parachute systems because wireless links in airborne environments may have limited bandwidth, unstable connectivity, and strict timing constraints.

Before mission deployment, the target stores and validates the certificate of the parachute PA_x . Therefore, the certificate is treated as a preloaded mission credential and is not transmitted in every online authentication message.

In the proposed AFAPS protocol, the transmitted message from PA_x to the target is

$$\{AID_x, P_x, Q_x, P_{mx}, T_x, Seq_x, N_x, C_x, \tau_x, S_x\}.$$

The encrypted mission payload is defined as

$$M_x = message_x \parallel DP_x \parallel Info_x \parallel T_x \parallel Seq_x.$$

To obtain a concrete communication overhead, a compact mission-payload format is considered. In this format, $message_x$ is 32 bytes, DP_x is 24 bytes, $Info_x$ is 32 bytes, T_x is 8 bytes, and Seq_x is 4 bytes. Therefore,

$$|M_x| = 32 + 24 + 32 + 8 + 4 = 100 \text{ bytes.}$$

Since AES-GCM does not increase the ciphertext length apart from the authentication tag, and the tag τ_x is counted separately, the ciphertext size is

$$|C_x| = |M_x| = 100 \text{ bytes.}$$

The fixed-size fields of the transmitted message are AID_x , P_x , Q_x , P_{mx} , T_x , Seq_x , N_x , τ_x , and S_x . Their total size is calculated as

$$32 + 33 + 33 + 33 + 8 + 4 + 12 + 16 + 32 = 203 \text{ bytes.}$$

Thus, the fixed authentication-related overhead is

$$203 \times 8 = 1624 \text{ bits.}$$

Accordingly, the total per-message communication cost of AFAPS is

$$C_{AFAPS} = 1624 + 8(100) = 2424 \text{ bits.}$$

Since

$$2424/8 = 303,$$

the total communication overhead of AFAPS is

$$C_{AFAPS} = 2424 \text{ bits} = 303 \text{ bytes.}$$

The communication cost comparison is presented in Table 5. For schemes whose payload size is fixed in the original studies, the reported total communication overhead is used. In addition, the bit values are converted into bytes to provide a more intuitive comparison.

Table 5. Communication cost comparison of AFAPS with related UAV/IoD authentication schemes.

Scheme	Scenario	Comm. Cost (Bits)	Comm. Cost (Bytes)
[20]	System login and authentication	1104	138
[28]	Drone-ground station authentication	2432	304
[29]	Soldier-drone authentication	1568	196
[30]	Drone-to-drone authentication	1856	232
[78]	Player-UAV-GCS authentication and communication	5536	692
AFAPS	Parachute-to-target encrypted mission-payload delivery	2424	303

As shown in Table 5, the proposed AFAPS protocol requires 2424 bits, namely 303 bytes, for one online authentication and encrypted mission-payload delivery message when the certificate is preloaded before the mission. This value includes the fixed authentication-related fields and a compact 100-byte encrypted mission payload. The result is slightly lower than Nyangaresi et al., which requires 2432 bits, namely 304 bytes, and significantly lower than Chen et al., which requires 5536 bits, namely 692 bytes, in the selected multi-party UAV communication phase.

Although Kirsal Ever, Choe and Kang, and Shariq et al. report lower communication overheads, AFAPS additionally transmits an encrypted mission payload containing the mission message, desired impact point, and information-replenishment data. Therefore, AFAPS provides not only authentication but also confidentiality for mission and target-location information within a compact single-message structure.

Overall, the proposed AFAPS protocol achieves low computational cost, avoids expensive bilinear pairing operations, and provides a compact communication structure while supporting authentication, integrity, freshness, and encrypted mission-payload confidentiality for autonomous parachute systems.

Figure 5 presents a combined visual comparison of the proposed AFAPS protocol and the selected UAV/IoD authentication schemes. For each scheme, the computational cost is shown in milliseconds using the left vertical axis, while the communication overhead is shown in bytes using the right vertical axis. This dual-axis representation is used because the two metrics have different units and numerical ranges. As shown in the figure, AFAPS achieves the lowest computational cost among the compared schemes. Its communication overhead is also comparable to lightweight UAV/IoD authentication schemes, while additionally carrying an encrypted mission payload containing the mission message, desired impact point, and information-replenishment data.

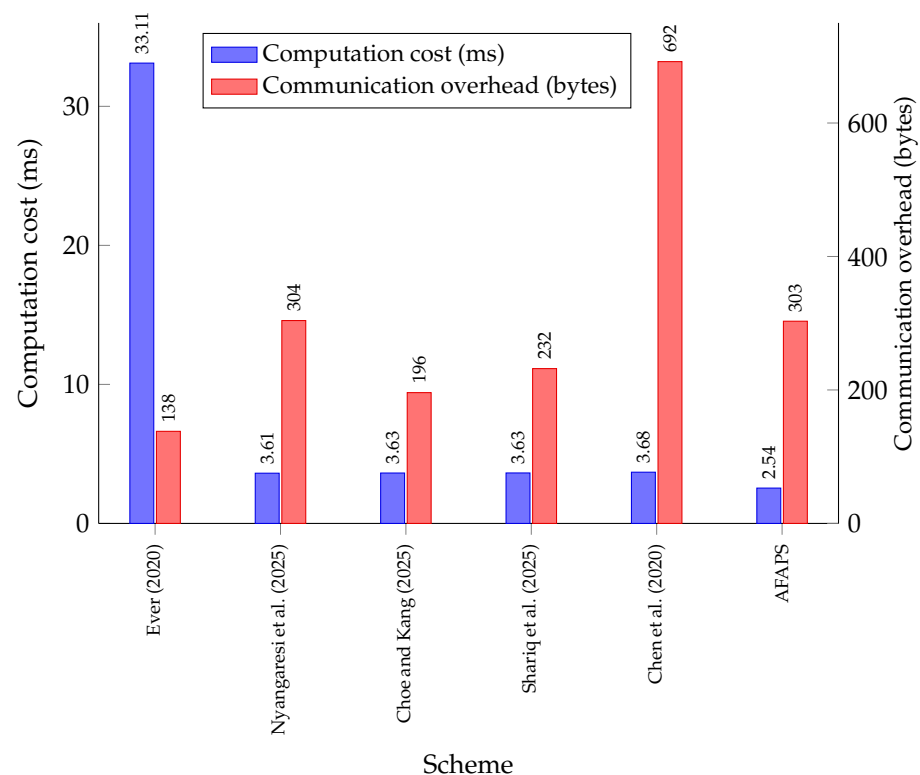


Figure 5. Performance comparison of AFAPS [20,28–30,78].

9. Conclusions

In this paper, the concept of information replenishment with autonomous ram-air parachute systems was investigated from a cybersecurity perspective. With this concept, autonomous parachute systems can be used not only for carrying physical supplies but also for securely delivering mission-critical information when conventional communication channels are unavailable, unreliable, or insecure. Since such systems may carry sensitive mission messages, desired impact-point data, and information-replenishment payloads,

securing the communication between the autonomous parachute and the target is critical for mission reliability and operational safety.

To address this requirement, an efficient, lightweight, and pairing-free ECC-based authentication framework, called AFAPS, was proposed. The AFAPS protocol provides certificate-based authentication, conditional identity privacy, traceability, replay protection, and encrypted mission-payload delivery. Unlike a purely signature-based authentication mechanism, AFAPS integrates ECDH-derived session-key establishment and AES-GCM authenticated encryption. Therefore, mission-related information is protected inside the encrypted payload and is not transmitted in plaintext.

The security of the proposed protocol was evaluated through an adversary model, informal security analysis, and BAN Logic-based formal analysis. In particular, the BAN Logic analysis shows that the target can authenticate the legitimate parachute, verify the freshness of the received authentication message, and accept the protected mission payload after successful cryptographic verification. These analyses indicate that AFAPS satisfies the main security requirements defined for the proposed information-replenishment scenario.

The performance evaluation indicates that AFAPS avoids costly bilinear pairing operations and provides a lightweight communication and computation structure suitable for resource-constrained autonomous parachute platforms. Future work will focus on embedded implementation, real device-level performance and energy measurements, and further optimization of the proposed framework for practical autonomous parachute deployments.

In future work, the proposed authentication framework can be extended by integrating trajectory-consistency verification and kinematic anomaly detection mechanisms based on the 6-DOF parachute model. Such an extension may enable the detection of GPS spoofing, abnormal trajectory deviations, or malicious manipulation attempts affecting the flight behavior of autonomous parachute systems.

Author Contributions: Conceptualization, B.C., Y.G.; methodology, B.C., Y.G.; software, B.C., Y.G.; validation, B.C., Y.G.; formal analysis, B.C., Y.G.; investigation, B.C., Y.G.; resources, B.C., Y.G.; data curation, B.C., Y.G.; writing—original draft preparation, B.C., Y.G.; writing—review and editing, B.C., Y.G.; visualization, B.C., Y.G.; supervision, B.C., Y.G.; project administration, B.C., Y.G. All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data supporting the reported findings are contained within the article. No external dataset was used. Additional details regarding the computational benchmark calculations are available from the corresponding author upon reasonable request.

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

References

1. Benney, R.; Barber, J.; McGrath, J. The joint precision airdrop system advanced concept technology demonstration. In Proceedings of the 18th AIAA Aerodynamic Decelerator Systems Technology Conference and Seminar, Munich, Germany, 23–26 May 2005.
2. Carrabba, P.L. *The Right Place at The Right Time—An Analysis of High Altitude Airdrop and The Joint Precision Airdrop System*; AFIT/GMO/ENS/04E-02; Air Force Institute of Technology: Dayton, OH, USA, 2004.
3. Xu, J.; Tian, W.; Kan, L.; Chen, Y. Safety assessment of transport aircraft heavy equipment airdrop: An improved STPA-BN mechanism. *IEEE Access* **2022**, *10*, 87522–87534.
4. Gramlich, D.; Hewing, L.; Scherer, C.W.; Preda, V.; Veenman, J.; Ardura, C.; Bennani, S.; Ebenbauer, C. Joint Trajectory and Tracking Controller Design Under Uncertain Models: Study with Autonomous Parafoils. *IEEE Trans. Control. Syst. Technol.* **2026**, *34*, 1465–1480.
5. Sun, H.; Sun, Q.; Sun, M.; Tao, J.; Chen, Z. Accurate modeling and homing control for parafoil delivery system based on wind disturbance rejection. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 2916–2934.

6. Yu, Z.; Sun, H.; Sun, Q.; Tan, P.; Chen, Z.; Qu, J. Dynamic path planning for parafoil homing in surface wind disturbance environment. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 15045–15059.
7. Fields, T.; Chance, A.; Nguyen, J. System Identification Techniques for a Micro-Scale Flap-Based Aerodynamic Decelerator System. In Proceedings of the 28th AIAA Aerodynamic Decelerator Systems Technology Conference, London, UK, 1–5 June 2026; p. 3832.
8. Zhang, M.; Hu, W.; Ji, S.; Song, Q.; Gong, P.; Kong, L. Vision-Assisted Landing Method for Unmanned Powered Parachute Vehicle Based on Lightweight Neural Network. *IEEE Access* **2021**, *9*, 130981–130989.
9. Boudreaux, L.; U.S. Army. *Airdrop of Supplies and Equipment*; TM 4-48.03/MCRP 4-11.3C/TO 13C7-1-11; U.S. Army Quartermaster School: Fort Lee, VA, USA, 2016. Available online: <https://www.scribd.com/document/368955570/TM-4-48> (accessed on 25 June 2026).
10. Chen, Z.; Xiang, X.; Ma, S.; Wu, Z.; Yang, J.; Li, R.; Li, Y.; Xi, Z. Research on Analysis and Predictive Modeling of the Frontal Flow Field During Parachutist High-Speed Descent. *Aerospace* **2026**, *13*, 211.
11. Wuest, M.R.; Benney, R.J. Precision Airdrop. In *Flight Test Techniques Series*; NATO Research and Technology Organization: Neuilly-sur-Seine, France, 2005; Volume 24.
12. Benney, R.; Meloni, A.; Cronk, A.; Tiaden, R. *Precision Airdrop Technology Conference and Demonstration*; AIAA: Reston, VA, USA, 2007.
13. Wegereef, W.; Jentink, H. *Precision Airdrop System SPADES*; NATO Research and Technology Organization: Neuilly-sur-Seine, France, 2006.
14. Genc, Y. A lightweight identity-based authentication scheme using elliptic curve cryptography for resource-constrained IoT devices. In *Next Generation Communication Networks for Industrial Internet of Things Systems*; CRC Press: Boca Raton, FL, USA, 2022; pp. 113–143.
15. Aljumah, A.; Ahanger, T.A.; Ullah, I. Challenges in Securing UAV IoT Framework: Future Research Perspective. *IEEE Trans. Netw. Serv. Manag.* **2025**, *22*, 2607–2629. <https://doi.org/10.1109/TNSM.2025.3554354>.
16. Poorvi, J.; Kalita, A.; Gurusamy, M. Reliable and Efficient Data Collection in UAV-Based IoT Networks. *IEEE Commun. Surv. Tutorials* **2026**, *28*, 2531–2571. <https://doi.org/10.1109/COMST.2025.3550274>.
17. Banafaa, M.K.; Pepeoglu, Ö.; Shayea, I.; Alhammadi, A.; Shamsan, Z.A.; Razaz, M.A.; Alsagabi, M.; Al-Sowayan, S. A Comprehensive Survey on 5G-and-Beyond Networks with UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges. *IEEE Access* **2024**, *12*, 7786–7826. <https://doi.org/10.1109/ACCESS.2023.3349208>.
18. Viana, J.; Farkhari, H.; Jimenez, V.P.G. Securing 5G and Beyond-Enabled UAV Links: Resilience Through Multiagent Learning and Transformers Detection. *IEEE Access* **2025**, *13*, 153993–154007.
19. Granelli, F.; Lu, Y.P.; Wu, Q.; Yuan, Z.; Abdalla, A.S.; Marojevic, V.; Jiang, Y.; Afghah, F.; Geraci, G.; Mukherjee, A.; et al. A Survey on Unmanned Aerial Vehicles (UAVs) Communications: State-of-the-Art, Existing Standards, and Future Directions. *IEEE Open J. Commun. Soc.* **2026**, *7*, 3000–3045. <https://doi.org/10.1109/OJCOMS.2026.3675046>.
20. Ever, Y.K. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* **2020**, *155*, 143–149.
21. Cordill, B.; Fang, D.; Xu, S. A Comprehensive Survey of Security and Privacy in UAV Systems. *IEEE Access* **2025**, *13*, 117843–117866. <https://doi.org/10.1109/ACCESS.2025.3583985>.
22. Oli, A.; Mahalal, E. UAV Security: Attacks, Defenses, and Open Challenges. *IEEE Access* **2025**, *13*, 215606–215635. <https://doi.org/10.1109/ACCESS.2025.3647023>.
23. Chaudhry, S.A.; Nebhen, J.; Irshad, A.; Bashir, A.K.; Kharel, R.; Yu, K.; Zikria, Y.B. A physical capture resistant authentication scheme for the internet of drones. *IEEE Commun. Stand. Mag.* **2021**, *5*, 62–67.
24. Wei, X.; Ma, J.; Sun, C. A Survey on Security of Unmanned Aerial Vehicle Systems: Attacks and Countermeasures. *IEEE Internet Things J.* **2024**, *11*, 34826–34847. <https://doi.org/10.1109/JIOT.2024.3429111>.
25. Lee, J.; Lee, M. Lightweight Mutual Authentication and Session Key Agreement for UAV Roaming in Multi-Fog Tactical Networks. *IEEE Access* **2026**, *14*, 89518–89534. <https://doi.org/10.1109/ACCESS.2026.3696703>.
26. Choi, J.; Kwon, D.; Son, S.; Park, Y.; Das, A.K.; Park, Y. A PUF-Based Lightweight Authentication Scheme for UAV-Assisted Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 13782–13798. <https://doi.org/10.1109/TITS.2025.3564581>.
27. Khan, M.A.; Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Shah, J.A.; Uddin, M.I.; Alsharif, M.H.; Algarni, F. A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3416–3425.
28. Nyangaresi, V.O.; Ahmad, M.; Maghrabi, L.A.; Althaqafi, T. Cost-effective PUF and ECC based authentication protocol for secure internet of drones communication. *IEEE Internet Things J.* **2025**, *12*, 33844–33857.
29. Choe, H.; Kang, D. ECC-based authentication protocol for military Internet of Drone (IoD): A holistic security framework. *IEEE Access* **2025**, *13*, 21503–21519.

30. Shariq, M.; Jamil, N.; Rawat, G.S.; Chaudhry, S.A.; Masud, M.; Das, A.K. Provably secure and reliable privacy-preserving authentication scheme for drone-to-drone communications in internet of autonomous things. *IEEE Trans. Mob. Comput.* **2025**, *25*, 1445–1456.
31. Genc, Y.; Afacan, E. Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). In *Proceedings of the 15th Aerodynamic Decelerator Systems Technology Conference*; AIAA: Reston, VA, USA, 2021; pp. 1–6.
32. Genç, Y.; Afacan, E. Implementation of New Message Encryption using Elliptic Curve Cryptography Over Finite Fields. In *Proceedings of the 2021 International Congress of Advanced Technology and Engineering (ICOTEN)*; IEEE: New York, NY, USA, 2021; pp. 1–6.
33. Zhang, A.; Xu, H.; Bi, W.; Xu, S. Adaptive mutant particle swarm optimization based precise cargo airdrop of unmanned aerial vehicles. *Appl. Soft Comput.* **2022**, *130*, 109657.
34. Jann, T.; Doherr, K.F.; Gockel, W. Parafoil test vehicle ALEX-Further development and flight test results. In *Proceedings of the 15th Aerodynamic Decelerator Systems Technology Conference*; AIAA: Reston, VA, USA, 1999; p. 1751.
35. Tao, J.; Sun, Q.; Zengqiang, C.; Yingping, H. Modeling and Simulation of Parafoil Systems in Wind Fields. In *Proceedings of the 11th Chinese Intelligent Systems Conference*; Springer: Cham, Switzerland, 2016; Volume 404, pp. 109–117.
36. Zhang, Z.; Zhao, Z.; Fu, Y. Dynamics analysis and simulation of six DOF parafoil system. *Clust. Comput. J. Netw. Softw. Tools Appl.* **2019**, *22*, 12669–12680.
37. Rimani, J. High Lift Systems For Planetary Descent And Landing. Master's Thesis, Politecnico di Torino, Turin, Italy, 2018.
38. Li, B.; He, Y.; Han, J.; Xiao, J. A new modeling scheme for powered parafoil unmanned aerial vehicle platforms. *Chin. J. Aeronaut.* **2019**, *32*, 2466–2479.
39. Chen, J.; Niu, W.; Ma, W.; Yang, M.; Wang, L.; Xi, H.; Song, J.; Fa, S.; Yang, S. Effective Prediction for the Landing Points of Airdroppable Underwater Vehicles Based on Dynamical Modeling. *IEEE J. Ocean. Eng.* **2025**, *51*, 254–269.
40. Hussain, S.; Chaudhry, S.A.; Alomari, O.A.; Alsharif, M.H.; Khan, M.K.; Kumar, N. Amassing the security: An ECC-based authentication scheme for Internet of drones. *IEEE Syst. J.* **2021**, *15*, 4431–4438.
41. Son, S.; Kwon, D.; Lee, S.; Jeon, Y.; Das, A.K.; Park, Y. Design of Secure and Lightweight Authentication Scheme for UAV-Enabled Intelligent Transportation Systems using Blockchain and PUF. *IEEE Access* **2023**, *11*, 60240–60253.
42. Teng, L.; Jianfeng, M.; Pengbin, F.; Yue, M.; Xindi, M.; Jiawei, Z.; Gao, C.; Di L. Lightweight security authentication mechanism towards UAV networks. In *Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA)*; IEEE: New York, NY, USA, 2019; pp. 379–384.
43. Alladi, T.; Bansal, G.; Chamola, V.; Guizani, M. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15068–15077.
44. Nyangaresi, V.O.; Ibrahim, A.; Abduljabbar, Z.A.; Hussain, M.A.; Al Sibahee, M.A.; Hussien, Z.A.; Ghrabat, M.J.J. Provably secure session key agreement protocol for unmanned aerial vehicles packet exchanges. In *Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*; IEEE: New York, NY, USA, 2021; pp. 1–6.
45. Genc, Y.; Aytas, N.; Akkoc, A.; Afacan, E.; Yazgan, E. ELCPAS: A new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV. *Veh. Commun.* **2023**, *39*, 100549.
46. Genc, Y.; Korkuc, C.; Aytas, N.; Afacan, E.; Sazli, M.H.; Yazgan, E. A Novel Identity-Based Privacy-Preserving Anonymous Authentication Scheme for Vehicle-to-Vehicle Communication. *Elektron. Elektrotehnika* **2023**, *29*, 69–77.
47. Asghar, Khan, M.; Ullah, I.; Kumar, N.; Afghah, F.; Barb, G.; Noor, F.; Alqahtany, S. A Certificate-Based Ring Signcryption Scheme for Securing UAV-Enabled Private Edge Computing Systems. *IEEE Access* **2024**, *12*, 83466–83479. <https://doi.org/10.1109/ACCESS.2024.3409359>.
48. Alzahrani, N. A Verifiably Secure and Lightweight Device-to-Device (D2D) Authentication Protocol for the Resource-Constrained IoT Networks. *IEEE Access* **2025**, *13*, 92982–92996. <https://doi.org/10.1109/ACCESS.2025.3568692>.
49. Zhang, X.; Wu, D.; Zhang, R. An ECC-Based Three-Factor Authentication and Key Management Protocol for Session Key Leakage Resilience in Internet of Drones. *IEEE Internet Things J.* **2026**, *13*, 11436–11445. <https://doi.org/10.1109/JIOT.2025.3647437>.
50. Liu, C.; Huang, T.; Ma, M. UAP: A System Authentication Protocol for UAV Relay Communication by UAV-Assisted. *IEEE Open J. Veh. Technol.* **2025**, *6*, 1539–1550. <https://doi.org/10.1109/OJVT.2025.3567079>.
51. Chauhdary, S.H.; Ma, T.; Jiang, L.; Khan, F.A.; Das, A.K.; Chaudhry, S.A. PUF-ILM: A PUF-Enabled Authentication Scheme for Internet of Vehicles Using Improved Logical Mapping. *IEEE Internet Things J.* **2026**, *13*, 13787–13800. <https://doi.org/10.1109/JIOT.2026.3656432>.
52. Korkuc, C.; Dogantuna, T.; Afacan, E.; Bostanci, E. Blockchain Based Network Access Control (NAC) Management Solution and Architecture. In *Proceedings of the 2021 29th Signal Processing and Communications Applications Conference (SIU), Istanbul, Türkiye, 9–11 June 2021*; IEEE: New York, NY, USA, 2021; pp. 1–4. <https://doi.org/10.1109/SIU53274.2021.9477893>.
53. Korkuc, C.; Genc, Y.; Dogantuna, T.; Afacan, E.; Dener, M. BBNAC: Blockchain-Based Network Access Control for IT/OT Infrastructures. *J. Netw. Syst. Manag.* **2026**, *34*, 60. <https://doi.org/10.1007/s10922-026-10033-w>

54. Korkuc, C.; Aytas Korkmaz, N.; Genc, Y.; Akkoc, A.; Afacan, E.; Yazgan, E. BLOCKBOX: Blockchain-Based Black Box Designing and Modeling. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8057. <https://doi.org/10.1002/cpe.8057>
55. Korkuc, C.; Genc, Y.; Afacan, E. Blockchain Technology and Cyber Security in Intelligent Transportation Systems. In *AIoT for Smart Transportation*; Institution of Engineering and Technology (IET): London, UK, 2025; Chapter 11, pp. 215–234. https://doi.org/10.1049/PBTR047E_ch11.
56. Arachchige, K.G.; Alkaabi, G.; Murtaza, M.; Haq, Q.E.U.; Abualkishik, A.Z.; Lee, C.-C. Threat Landscape and Integrated Cybersecurity Framework for V2V and Autonomous Electric Vehicles. *World Electr. Veh. J.* **2025**, *16*, 469. <https://doi.org/10.3390/wevj16080469>.
57. Yapici, A.T.; Abut, N. An Intelligent and Secure IoT-Based Framework for Predicting Charging and Travel Duration in Autonomous Electric Taxi Systems. *Appl. Sci.* **2025**, *15*, 12423. <https://doi.org/10.3390/app152312423>.
58. Wang, J.; Wang, S.; Wen, K.; Weng, B.; Zhou, X.; Chen, K. An ECC-Based Authentication Protocol for Dynamic Charging System of Electric Vehicles. *Electronics* **2024**, *13*, 1109. <https://doi.org/10.3390/electronics13061109>.
59. El-Hajj, M. Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. *Electronics* **2024**, *13*, 3941. <https://doi.org/10.3390/electronics13193941>.
60. Mbachu, U.M.; Fatima, R.; Sherif, A.; Dockery, E.; Mahmoud, M.; Alsabaan, M.; Khalil, K. Hardware Acceleration-Based Privacy-Aware Authentication Scheme for Internet of Vehicles Using Physical Unclonable Function. *Sensors* **2025**, *25*, 1629. <https://doi.org/10.3390/s25051629>.
61. Elhadad, M.K.; Gebali, F. Mutual V2I Multifactor Authentication Using PUFs in an Unsecure Multi-Hop Wi-Fi Environment. *Electronics* **2025**, *14*, 4167. <https://doi.org/10.3390/electronics14214167>.
62. Kim, H. Efficient and Scalable Authentication Framework for Internet of Drones (IoD) Networks. *Electronics* **2025**, *14*, 2435. <https://doi.org/10.3390/electronics14122435>.
63. Zou, W.; Guo, Q.; Xie, X. A Certificateless Aggregated Signcryption Scheme Based on Edge Computing in VANETs. *Electronics* **2025**, *14*, 1993. <https://doi.org/10.3390/electronics14101993>.
64. Wu, W.; Xiang, L.; Yang, K. A Camera-Cooperative ISAC Framework for Multimodal Non-Cooperative UAVs Sensing. *IEEE J. Sel. Top. Signal Process.* **2026**. <https://doi.org/10.1109/JSTSP.2026.3705654>.
65. Semenov, S.; Krupska-Klimczak, M.; Mazurek, P.; Zhang, M.; Chernikh, O. Improving Unmanned Aerial Vehicle Security as a Factor in Sustainable Development of Smart City Infrastructure: Automatic Dependent Surveillance–Broadcast (ADS-B) Data Protection. *Sustainability* **2025**, *17*, 1553. <https://doi.org/10.3390/su17041553>.
66. Cacan, M. Adaptive Control of Autonomous Airdrop Systems in Degraded Conditions. Ph.D. Thesis, Georgia Institute of Technology, Atlanta, GA, USA, 2016.
67. Kaminer, I.I.; Yakimenko, O.A. Development of control algorithm for the autonomous gliding Delivery system. In *Proceedings of the 17th AIAA Aerodynamic Decelerator Systems Technology Conference and Seminar, Wichita, KS, USA, 19–22 May 2003*; AIAA: Reston, VA, USA, 2003.
68. Puskas, E. Ram air parachute design considerations and applications. In *Proceedings of the 8th Aerodynamic Decelerator and Balloon Technology Conference, Hyannis, MA, USA, 2–4 April 1984*; AIAA: New York, NY, USA, 1984.
69. Toohey, D. Development of a Small Parafoil Vehicle for Precision Delivery. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2005.
70. Wang, J.; Xiong, Z.; Zhao, Y.; Ding, Y.; Liu, Y.; Wang, H.; Yan, L. Covariance matrix transformation method for absolute/relative measurements fusion of vision/IMU/GNSS integration in parafoil landing. *IEEE Sensors J.* **2024**, *24*, 16673–16687.
71. Lins, F.A.A.; Vieira, M. Security Requirements and Solutions for IoT Gateways: A Comprehensive Study. *IEEE Internet Things J.* **2021**, *8*, 8667–8679. <https://doi.org/10.1109/JIOT.2020.3041049>.
72. Hankerson, D.; Menezes, A. Elliptic curve cryptography. In *Encyclopedia of Cryptography, Security and Privacy*; Springer: Boston, MA, USA, 2021; pp. 1–2.
73. Xiong, W.; Wang, R.; Wang, Y.; Zhou, F.; Luo, X. CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3456–3468.
74. Dogantuna, T.; Korkuc, C.; Genc, Y.; Dener, M.; Afacan, E. BB-API: A Secure and Transparent Blockchain-Based Model for Enterprise API Key Management. In *Proceedings of the 2026 8th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Türkiye, 21–23 May 2026*; pp. 1–7. <https://doi.org/10.1109/ICHORA69329.2026.11537165>.
75. Korkuc, C.; Dogantuna, T.; Genc, Y.; Afacan, E.; Dener, M. A Blockchain Attestation Layer for Zero Trust Network Access. In *Proceedings of the 2026 8th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Türkiye, 21–23 May 2026*; pp. 1–6. <https://doi.org/10.1109/ICHORA69329.2026.11537007>.
76. Choi, J.; Park, Y. A Secure Authentication Scheme for Hierarchical Federated Learning with Anomaly Detection in IoT-Based Smart Agriculture. *Appl. Sci.* **2026**, *16*, 3211.

77. Lee, S.; Son, S.; Kwon, D.; Park, Y.; Park, Y. A secure and efficient authentication scheme for fog-based vehicular ad hoc networks. *Appl. Sci.* **2025**, *15*, 1229.
78. Chen, C.L.; Deng, Y.Y.; Weng, W.; Chen, C.H.; Chiu, Y.J.; Wu, C.M. A traceable and privacy-preserving authentication for UAV communication control system. *Electronics* **2020**, *9*, 62.
79. Lynn, B. PBC (Pairing-Based Cryptography) Library. 2022. Available online: <https://crypto.stanford.edu/pbc/> (accessed on 5 July 2026).
80. Granlund, T.; The GMP Development Team. GNU MP: The GNU Multiple Precision Arithmetic Library, Version 6.3.0. 2024. Available online: <https://gmplib.org/> (accessed on 5 July 2026).

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