

國立成功大學

交通管理科學系碩士在職專班

碩士論文

防止無人機影響機場飛行安全之策略

Strategies of protecting airport safety from accidental or malicious UAV

operations



研究生：陳炫旻

指導教授：陳文字 博士

中 華 民 國 一 百 一 十 一 年 一 月

論文審查及口試合格證明

國立成功大學

碩士在職專班論文

防止無人機影響機場飛行安全之策略

Strategies of protecting airport safety from accidental or
malicious UAV operations

研究生：陳炫旻

本論文業經審查及口試合格特此證明

論文考試委員：

鄭 泉 評
林 珮 君
盧 筱 涵
陳 文 豪

指導教授：

陳 文 豪

單位主管：

邵 永 祥

(單位主管是否簽章授權由各院、系(所、學位學程)自訂)

中 華 民 國 111 年 1 月 22 日

摘要

無人機現今蓬勃發展，目前又因疫情關係，在國外一群無人機愛好者利用他們的飛行操控技能，替居家隔離患者提供藥品及食物無接觸遞送服務。使得無人機在生活中的運用越來越廣泛了，當無人機越來越頻繁則會造成飛航安全的問題，中央或地方政府必須劃定的管制區內進行活動時，也需透過系統提出申請，才能在合法區內依規定操作飛行。

在以前反制無人機極為困難，傳統防空系統主要用於反制飛機或飛彈的攻擊，雖然技術層次日益精進，成本也大幅增加，世界各國均加快發展、測試及部署無人機反制系統，以因應此種新興的不對稱威脅。本研究是針對機場的禁航區域用反制小型無人機的策略，提供給未來研究防止無人機技術參考方向。

此研究是將反制無人機系統分為三種策略，分別為監管策略、干擾策略及摧毀策略，從無人機遙控器的無線頻段(2.4G、5.8 及 GPS)去探討監控管理、無線干擾以致最後都無法侵入時以摧毀手段，可以了解無人機與遙控器構連時的程序，並研究此程序的步驟。

其中對於干擾策略則計算無線電的自由空間、飽和度及 EIRP，將上述的頻段以公式算出功率，針對市面上無人機干擾槍發射功率與距離大小作為未來研究干擾槍相關距離與功率關係；但也必須依循 NCC 的低功率射頻電機技術規範，因此發射功率大小均須先行提出申請。

關鍵詞：反制無人機、自由空間傳播模型、等效輻射功率、電波干擾

Extended Abstract

Strategies of protecting airport safety from accidental or malicious UAV operations

Master Student : Hsuan-Ming Chen

Adviser : Wen-Tzu Chen

Department of Transportation and Communication Management Science, National Cheng Kung University

SUMMARY

Drones are booming. Due to the epidemic, a group of drone enthusiasts abroad use their flight control skills to provide contactless delivery services for medicines and food for home quarantined patients. The use of drones in life is becoming more and more extensive. When drones become more frequent, they will cause flight safety problems. When activities are carried out in the control area that the central or local government must delineate, raising the issue through the system is also necessary. After the application is approved, the flight can be operated within the legal area under regulations. In the past, it was challenging to counter UAVs. Traditional air defense systems were mainly used to counter the attacks of aircraft or missiles. Although the technical level has become increasingly sophisticated and the cost has also increased significantly in countering small UAVs, in order to counter UAV threats, the countries in the world are accelerating the development, testing, and deployment of UAV countermeasures to counter this emerging asymmetric threat. This research is a strategy for using anti-UAV in the no-navigation area of the airport. In addition, the study provides a reference direction for future research on anti-UAV technology. This thesis divides the anti-UAV system into three strategies. From the wireless frequency band (2.4 GHz, 5.8 GHz, and GPS) of the drone remote control to discuss the monitoring management, wireless interference, and finally destroy the method when the intrusion is impossible. From the figure below, we can understand the procedure when the drone connects with the remote controller. Among them, the free space propagation loss, receiver saturation, and

EIRP of the radio are calculated for the jamming strategy. The power of the above frequency bands is calculated by a formula, which can be used for the transmission distance of drone jamming guns on the market. In addition, NCC's low-power RF device specification must be followed to comply with related regulations.

Keywords: Counter UAV, Radio Free Space, EIRP, NCC

INTRODUCTION

In recent years, the development of Unmanned Aerial Vehicles (UAVs) has become increasingly vigorous. UAVs combined with artificial intelligence (AI) technology can be used in photography, security inspections, freight, and agricultural spraying.

Due to improper use or malicious use by people with intentions, it affects public safety. The airport's surrounding area is an area where aircrafts take off and land frequently. Any floating objects and obstacles may pose a potential threat to the flight safety of takeoff and landing aircrafts. It is important to elevate the homeland security level and consider the security issues arising from drone's various use scenarios or malicious use. National security and public safety are the prerequisites for everything. The government must take into account the protection of individual rights and legitimate activities at the same time.

MATERIAL AND METHOD

The Civil Aviation Law (Activity Area) defined the meaning of the three colors of "red, yellow, and green" in the airspace map. The Civil Aviation Administration explained that the green area represents the legal activity. Whether natural or legal, as long as they comply with the operating regulations, they can engage in remote control drone activities. The legal person can also apply for an activity permit to exclude restricted items and fly at night or over crowds of assemblies and parades.

The anti-UAV technology system consists of three major parts: 1) detection, tracking, and early warning technology, 2) interference technology, and 3) destruction technology. In addition, there are active anti-UAV technical means, passive camouflage protection methods, and active and passive anti-UAV technology. The synthesis of the anti-UAV combat effect makes the overall maximum and optimization.

RESULT AND DISCUSSION

The first regulatory control strategy is the follows. The regulatory type is the most complex and the easiest to crack. Because of the initial pairing process in the wireless connection step, the radio's remote control must be built before controlling the drone. After the pairing process, any intruder cannot hack and interfere with the pairing ID. This strategy not only requires blocking the control

signal of the UAV without damaging the UAV itself but also needs to realize the camouflage and deception on the control command.

- Second strategy, wireless jamming: The first step is to interfere with the frequency band of the flight controller of the wireless receivers, including 2.4 GHz and 5.8 GHz frequency bands. If we can't interfere with the above two frequency bands, then interfering with the GPS band must be used. GPS interference makes the drone go back to its takeoff place or disable the flight. It is required to complete the blocking of the UAV control signal without damaging the UAV itself and to realize camouflage and deception on the control command. The interference strategy is to use radio interference

- The third strategy, destruction: The strategy is to directly destroy UAV using missile technology, laser weapon technology, microwave weapon technology, force-based UAV technology, and conventional fire destruction technology.

Three strategies are used and the calculation formula is used to calculate the maximum power and saturation distance for frequency bands of 2.4G, 5.8G and GPS. Using the formula, we can calculate the required interference power of the jamming gun for the corresponding type of UAV. Because of the transmission power limitation, the power of the jamming gun and the interference distance are very small.

According to the current specification of the jamming gun, the relationship between distance and power can be calculated. The result can also be used as the direction and basis for the future research.

CONCLUSION

Our government should list drone confrontation as one of the essential national constructions. Therefore, combined with the relevant technologies and resources of the Chinese Academy of Sciences and civil society, the multi-level construction of the airport UAV air defense system should be deployed to reduce the response time and costs.

誌謝

從 2018 年 1 月份選修學分班課程開始，到今年(2022 年 1 月)也過了四年時間，雖然自己已取得南台科技大學資管所碩士學位，但為了自己能擁有通信的碩士學位還是考進成大交通管理暨電信管理研究所，每天都是忙碌的喜悅，在完成論文的過程中，首先要感謝指導教授陳文字老師，老師跟我不只是師生而已，也是我在學習通信領域與生活中最重要的朋友，從不吝嗇也毫無保留的分享他的學習經驗，從我進碩士專班以來，一路引導我到完成學業，花了相當多的心思在我的論文上，逐字斧正，讓我能不斷地精益求精。特別感謝審查委員林珮琚老師、盧筱涵老師和鄭泉坪老師，在百忙之中撥冗對我的論文細心審閱並給予我很寶貴的意見，使我的論文更趨完善。感謝交管所指導過學生的老師們，您的教導開拓了我的思維，讓視野更開闊。

感謝給我最大支持力量的老婆雪萍，因為我是軍人職業且為了要讓我自己能於退伍後能有更多的養分與經驗，感謝妳讓我去念第二個碩士，在這麼長的時間裡的包容與付出，幫我照顧兩個小孩與我母親，讓我無後顧之憂，順利完成學業。最後，祝福 各位平安順利，再一次謝謝大家！

炫旻 謹誌

於成大 民國一百一十一年一月

目錄

論文審查及口試合格證明.....	I
摘要	I
EXTENDED ABSTRACT.....	III
誌謝	VI
表目錄	X
圖目錄	XI
第一章 緒論	1
1.1 研究背景	1
1.2 研究動機與目的	3
1.3 論文架構	5
第二章 背景與文獻回顧.....	6
2.1 無人飛行載具的定義	6
2.1.1 無人飛行載具	6
2.1.2 無人飛行載具系統	7
2.1.3 無人飛行載具之類型	8
2.2 無人飛行載具闖入禁區	9
2.2.1 禁區定義	9
2.3 反制無人飛行載具	12
2.3.1 反制無人飛行載具發展	13
2.3.2 反制無人飛行載具分類	13
2.4 通訊的干擾類型	14
2.4.1 無人飛行載具無線電通信頻段	15
2.4.2 無線電通信展頻	16
2.4.3 GPS 原理	17

2.4.4 GPS 干擾原理.....	18
2.5 文獻歸納	19
第三章 研究方法.....	21
3.1 研究系統架構(監控管制類型).....	21
3.1.1 理論依據(無人飛行載具控制器配對).....	21
3.1.2 理論依據(遙控器信號解譯).....	22
3.1.3 理論依據(無線加解密)	24
3.2 研究系統架構(無線干擾類型).....	24
3.2.1 理論依據(無線電干擾射頻自由空間).....	25
3.2.2 理論依據(無線電射頻等效全向性輻射功率).....	28
3.2.3 理論依據(干擾阻斷 GPS 類型).....	30
3.2.4 無人飛行載具干擾槍.....	32
3.3 反制無人飛行載具(摧毀類型評估).....	34
3.3.1 理論依據	34
第四章 研究結果.....	36
4.1 反制無人飛行載具監管策略.....	36
4.1.1 監管策略(無線遙控配對).....	36
4.1.2 監管策略(無線解密困境).....	37
4.2 反制無人飛行載具干擾策略	37
4.2.1 反制無人飛行載具無線電阻斷策略(自由空間)	39
4.2.2 反制無人飛行載具無線電阻斷策略(等效全向輻射功率).....	42
4.2.3 反制無人飛行載具 GPS 導航失效策略	42
4.3 反制無人飛行載具直接摧毀策略.....	43
第五章 結論與展望.....	46
5.1 結論	46

5.2 展望	46
參考文獻	47



表目錄

表 1、802.11a/b/g 接收器前端規範.....	28
表 2、全球所有衛星數量.....	31
表 3、無人飛行載具干擾槍規格.....	33
表 4、2.4G 發射功率與距離.....	40
表 5、5.8G 發射功率與距離.....	41
表 6、GPS 1575M 發射功率與距離.....	43



圖目錄

圖 1、無人飛行載具構連.....	1
圖 2、無人飛行載具的空域圖資.....	11
圖 3、飛行場四周禁止從事遙控無人機活動距離範圍.....	11
圖 4、機場四周禁止施放有妨礙飛航(行)安全距離範圍.....	12
圖 5、2.4G 頻段碼框圖.....	15
圖 6、反制無人飛行載具的原理圖.....	18
圖 7、無人飛行載具遙控訊號構連圖.....	22
圖 8、直接序列展頻與跳頻展頻.....	23
圖 9、無線通訊鏈路.....	26
圖 10、IP3 是三階截斷點.....	27
圖 11、無線通訊環境電波訊號.....	30
圖 12、無人飛行載具干擾槍.....	33
圖 13、遙控器與無人飛行載具配對圖.....	37
圖 14、無人飛行載具干擾欺騙策略圖.....	38
圖 15、無人飛行載具無線飛控干擾圖示.....	39
圖 16、船艦的反火箭系統圖示.....	44
圖 17、船艦的雷射武器系統圖示.....	44
圖 18、捕捉型無人機.....	45

第一章 緒論

1.1 研究背景

近期因無人飛行載具技術成熟軍用、民用無人飛行載具市場的迅速發展，無論是在軍事作戰體系及反恐行動中針對無人飛行載具系統的部署情況，還是非戰場環境下出於對機場、塔台軍事設施、海關及監獄等敏感區域安全考量，反制無人飛行載具技術也越來越受到重視，也將成為完整空中防禦中不可或缺的部分。由於無人飛行載具是新興科技，雖然非常方便，但也可能因未注意或駭客惡意入侵，影響公共安全，機場四周屬航機起飛與降落頻繁地區，任何漂浮體、障礙體均可能對起飛與降落航空載具之飛航安全造成威脅，闖入機場安全區域的遙控型無人飛行載具，除增加了危害飛航安全不確定因素外，也影響到飛航安全與機上乘客的權益，並造成無謂的油耗、航空安全及時間浪費，所以只能讓空中的在空機與地上的航機等待，待無安全疑慮方可放行，如圖 1 所示，無人飛行載具構聯圖。

過去偶有因民眾於機場附近遙控商用無人飛行載具(含空拍機)、天燈或放風箏，影響航空載具飛航安全，對飛安造成巨大影響，甚至對國家安全形成威脅。所以，此議題必需提至國家安全層級，思考無人飛行載具使用情境或惡意運用無人飛行載具所衍生安全問題。國家安全與公共安全為基礎，政府單位須同時對於個人權益與合法使用保障。

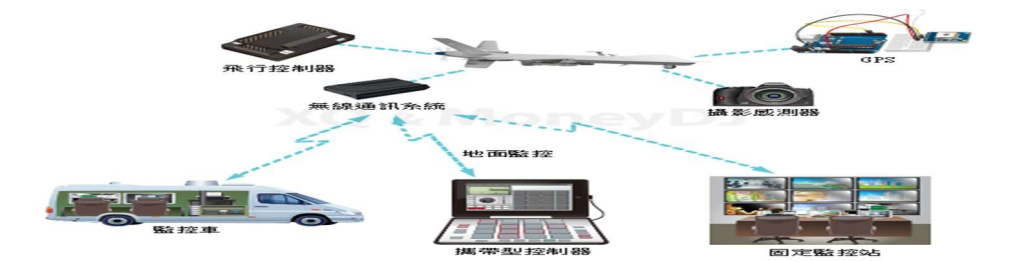


圖 1、無人飛行載具構連

(資料來源：本研究整理)

從技術層面上，要想對商用無人飛行載具進行有效管控，首先要能夠做到對無人飛行載具全方位、全天候的監控與探測。我們瞭解此類無人飛行載具在低空飛行時，機身與地面遙控的資料回傳通常需要藉助通訊及控制信號鏈路導航訊號。因此，我們可以利用全球定位系統（英語：Global Positioning System，通常簡稱 GPS），又稱全球衛星定位系統對無人飛行載具進行定位與追蹤後，對其進行干擾，使無人飛行載具自控系統混亂，無法獲得準確自身 GPS 座標，且與遙控器裝置的無線電通訊發生鏈路干擾，最終導致迫降、墜落或返航。中央科學研究院因此問題發明了反制無人飛行載具系統(包含無人飛行載具干擾器可以有效干擾 GPS 與 ISM 訊號)，此系統使用干擾方式對目標物(非法無人機)訊號頻率進行干擾，並不會影響到周圍頻率訊號。此系統採用訊號分析技術與干擾功能，配以無線電及定向儀干擾，可在較大範圍進行偵查，一旦發現問題，便可中斷無人飛行載具與其操作人員之間的聯絡並追蹤到無人飛行載具操控者位置，以便於實施管制或抓捕行動。除訊號與 GPS 干擾外，國外無人飛行載具反制技術包括雷射炮擊落與混合型技術等幾大類。

相關無人機新聞包含亞美尼亞和亞塞拜然發生領土糾紛，亞塞拜然多次使用無人機攻擊亞美尼亞軍隊，並獲得豐碩戰果。此役再度驗證無人機的實戰價值，廉價、容易購買的小型無人機，已成為繼遍布伊拉克與阿富汗的自製爆裂物之後，對中東地區美軍最嚴重威脅，呼籲五角大廈必須著手研擬反制方法和裝備，保護美軍人員免於小型無人機威脅。由於無人機技術愈來愈成熟，易於獲取且有利於武器化的世界中，是各國軍隊很可能面對的難題[1]。

無人機可以成群飛行，也可互相通聯、攜帶武器，甚至可以反制傳統的電波干擾技術，葉門叛軍「青年運動」使用伊朗提供的無人機，攻擊沙烏地阿拉伯第二大油田與最大煉油廠，爆炸後冒出熊熊大火。兩處石油設施遇襲後暫停生產作業，導致沙國每日原油產量減少約570萬桶，國際油價因此飆升。反制肆無忌憚的無人機已成為刻不容緩的任務[2]。

從行政監管方面，目前我國已採取規範無人飛行載具製造、無人飛行載具實名登記、設定敏感禁飛區域等，將無人飛行載具的防範工作列為安全保衛工作重要的課題，我國交通部已於110年11月29日發布遙控無人飛行載具管理規則。此外，世界各國也針對此問題律定相關政策法規。例如，英國對無人飛行載具使用做出規範，要求小型無人飛行載具必須時時刻刻在操作員的可視範圍內且操作員能對此無人機完全的掌控，在飛行時應與建築、其他形式飛行器(或天燈等)、車輛等及人群保持相當距離，以避免碰撞事故發生。

近年來無人飛行載具玩家越來越多，運用也越廣泛，民航局除透過修法管制外，機場四周禁止無人飛行載具釋放範圍，大約有 400 平方公里，無法只靠航空站及航空警察進行取締，民航局除了與軍方和國安單位共同合作，成立區域聯防機制，也必須靠硬體設備補足，讓不少台灣業者，看好反制型無人飛行載具需求。

本研究將探討防止無人飛行載具影響機場飛行安全，以反制無人飛行載具的方法在國際上有「軟體入侵方式」以干擾控制通訊及控制信號方式來反制無人飛行載具；「硬殺方式」則以摧毀無人飛行載具方式等 2 種手段，此研究以可行性評估與技術層面探討反制無人飛行載具的各種方式透過蒐集文獻，結合重要度可行性分析，以獲取當前須優先執行的策略。

1.2 研究動機與目的

因應遙控無人飛行載具活動漸漸增加，為能方便管理，交通部及民用航空局借鏡美國、日本、韓國及歐盟等國家的立法經驗與國際各國民航組織規範下，並考量國內目前環境與利害關係人意見，並融合社會秩序、公共安全及飛航安全並兼顧國家相關產學發展，在推動於「民用航空法」中增加遙控無人機專章及授權法規命令規範修法。其中遙控無人機專章修正草案自 109 年 3 月 31 日正式施行，而中華民國 110 年 11 月 26 日交通部交航字第 1100034924 號令修正發布第 41 條之 1，並於 110 年 11 月 29 日施行修正發布「遙控無人機管理規則」[3]。

無線電頻段干擾必須依據 NCC(國家通訊傳播委員會)【電波監理業務管理辦法】規定，第五條規定 8.3 kHz 至 3 THz 之各業務頻率之分配，應依行政院指定機關公告之中華民國無線電頻率分配表（以下簡稱頻率分配表）辦理。為整體電信及資訊發展之需要，頻率應和諧有效共用，前項頻率分配表由行政院指定機關定期檢討修定公告之；另第十條依頻率分配表規定，得在同一特定頻帶內，以不發生妨害性干擾為條件使用之業務，不得要求保障不受妨害性干擾。衛星陸地行動業務之陸地行動地球電臺，於必要時得與衛星水上行動電臺及衛星航空行動電臺通信[4]。

隨著無人機的擴散，美國執法部門與國家安全機構的反制無人飛行載具需求激增。美國國會意識到這個問題，並且在 2017 年與 2018 年的國防授權法案（National Defense Authorization Act for Fiscal Year, NDAA）中[5]，向國防部與能源部提供了反制無人飛行載具系統（Countermeasure Unmanned Aircraft System, CUAS）的部分許可權。小型無人飛行載具系統（Unmanned Aircraft System, UAS），通常被稱為無人機或無人飛行載具，在為民眾帶來生活便利的同時，同樣被也國內犯罪分子與恐怖分子利用，為國家安全造成很大的傷害。其中，一些犯罪分子使用無人機將毒品偷運到邊境或監獄，或是未經批准的無人機飛越體育場館與機場附近的控制空域、甚至撞到 101 大樓及闖入松山機場禁航區等等事件[6]，都暴露敏感設施與關鍵基礎設施在無人飛行載具面前的脆弱性，及國家執法與安全機構能力的嚴重的缺失[7]。

因此反制無人飛行載具系統變成一個很重要的事情，對於小型無人飛行載具系統在離地 10 公尺的低空域飛行時，則可運用干擾器或捕捉器實施癱瘓或攔捕。超過 10 公尺以上，可運用干擾器或防衛武器給予癱瘓或擊落，無人飛行載具的反制與規範可從技術層面與行政監管兩方面同時入手，有效降低其對社會造成的威脅，本研究以技術層面為主探討反制無人飛行載具闖入禁區方法，讓無人飛行載具癱瘓或失效。故本研究目的為：

1. 先從軟體方法或硬體方法探討飛航安全，探討無人飛行載具闖入禁區之影響安全。

2. 研擬無人飛行載具飛行之通訊控制信號及 GPS 定位相關技術。
3. 研擬防制無人飛行載具闖入禁區的方法。
4. 評估防制方法的挑戰。

1.3 論文架構

本論文第一章將介紹無人飛行載具氾濫的嚴重性與影響飛航安全的重要性，並說明無人飛行載具為何會影響飛航安全，最後歸納出本研究之動機，第二章介紹交通部民用航空局對於無人飛行載具相關法律規範及依據及禁區，並以反制無人飛行載具框架下相關三種類別為基礎，介紹相關技術層面及可行性評估與本研究所使用到的各種干擾方法及案例，最後對於過往文獻做個歸納與結語。第三章說明整體研究系統架構，接著介紹依架構評估三種策略的理論依據及對於干擾槍的規格說明。第四章針對三種類型依照第三章的理論與方程式計算出 2.4G、5.8G 及 GPS 無線訊號可干擾距離及功率，並說明各系統之可行性與窒礙問題。第五章說明可運用方程式計算出干擾槍的功率大小與干擾範圍，但干擾槍亦要合於規範方可干擾，提供無人機進入禁區時的策略，未來研究參考依據。

第二章 背景與文獻回顧

本章節會將本研究中所使用技術做詳細的討論，其中包含了解飛行安全無人飛行載具、禁制區律定規範、如何禁止非法無人機進入禁航區的策略(例如：監管控制類、干擾阻斷類及直接摧毀類)等部分，最後統整文獻並做出歸納。

2.1 無人飛行載具的定義

無人飛行載具(Unmanned Aerial Vehicle，縮寫：UAV)或稱為無人機系統(Unmanned Aircraft System，縮寫：UAS)，俗稱無人機、無人飛機及無人作戰飛機，廣義為不需要駕駛者駕駛各類飛行器，在用途上分為軍用與民用。至於無人駕駛的作戰飛機則是具備類似攻擊型的飛機，但沒有駕駛者可以發起攻擊，且成本較低。

2.1.1 無人飛行載具

無人飛行載具也稱遙控駕駛航空載具或無人航空載具，是一種以無線電遙控器設備或預設程式操縱無人機的飛行器。無人飛行載具機動及靈活特色，體積較小及重量較輕，可隨時攜帶與運輸。對起飛與降落的要求較低，可隨時起飛及降落。商用的無人飛行載具僅能低空平穩地飛行，可彌補衛星定位遙控與航空攝影時，受雲層遮擋而影像回傳失真。除了上述的商用外，也常使用在軍事用途，無人飛行載具替代了飛行員執行高風險的任務。特別在近幾年國際上經常被非常大量地使用無人飛行載具執行作戰，可預見未來的戰場上無人飛行載具用途將越來越多，且已成為各國家軍事武器研發重點方向[8]。同時，無人飛行載具作為一種技術高、機動性高、無需人員在飛行載具上執行高風險任務，在民用領域亦可完成防災減災用途、警用高速公路巡查、農藥噴灑、地震勘查、海事巡邏、森林區防火等多種任務。

依國軍無人駕駛航空載具系統空域管制作業程序第2點第2項對其定義，無人飛行載具之定義指具有動力、使用航空動力提供載具上升、不載人(含駕駛操作員)、能遙控操控飛行或自動飛行、可掛一般彈頭或載毀滅性、在軍事戰略上可回收或直接耗損的無人機。

然依民用航空法修正草案第 2 條第 26 項對遙控中無人飛行載具所為之定義：指從遙控設備用通信鏈路進行飛航控制無人航空載具。根據國際民航組織(以下簡稱 ICAO) RPAS Manual Draft 的定義為「遙控駕駛之航空載具定義：遙控駕駛航空載具 (RPA)：一架由遙控站操縱的無人駕駛航空載具」。

2.1.2 無人飛行載具系統

無人飛行載具系統的遙控方面則定義無線電資料上、下鏈(圖資)傳輸介面的地面控制站(Ground Control Station，縮寫：GCS)為完整系統。GCS 則可依設計方法或需求面形成任何形式，如：地面的簡易 GCS、地面的箱型、車載型的手持式等。

無人機中的自動飛行系統內包含一套衛星導航裝置、偵測器、繫盤功能、氣壓高度計、電腦作業系統及設計飛行的軟體等，無人機飛行操作上則採取遙控或自主控制模式，其飛行操作一般包括四種類型：

- 一、由地面人員在視距內操作飛行。
- 二、由控制人員在視距外操作飛行。
- 三、包含預先路徑規劃的程式控制進行自動飛行。
- 四、透過地面人員追蹤器，讓無人機自動追隨運動中的人員（或車輛）飛航。

無人飛行載具通常包含地面飛控系統、發射後回收系統及無人飛行載具系統等三個次系統：

- 一、地面飛控系統：地面的控制系統包含，監控人員、地面飛行操控或地面即時解讀人員與資料分析；硬體設備方面包括指令的傳送與訊號接收及發射及情報資訊的分析與接收等，本研究則是針對此次系統探討出三個策略，對於飛控系統進行干擾策略。

二、發射／回收系統：

- (一)在發射方面，除了傳統長跑道等待飛行外，因受地形地物相關影響（如沙漠、河床、山谷）可以以彈射軌發射或火箭方式助推及人力方式拋射等。

(二)降落與回收方面除長跑道降落外，亦有運用纜線勾鎖、降落傘方式或攔截網方式回收。

三、飛行載具系統：飛行載具的系統包括，外型與機體結構、自動駕駛與推進系統、資料鏈、特定任務酬載裝備及資料儲存系統及導航設備。

2.1.3 無人飛行載具之類型

無人機一般有軍用、民用、商用、工業與消費性..等類型之分，其與傳統飛機互相比較，具有機動靈活、成本低、隱蔽性好、彈性大、地域限制低及支援裝備較少等相關特色。然而無人飛行載具依其載具形狀、大小、飛行距離、外型、功用、特性與飛行速度、航時、任務功能等，大致上可以分成幾個不同的類型，以下對不同類型分別敘述說明：

一、依形狀、大小、飛行距離區分：

(一)微型無人飛行載具 (Micro Aerial Vehicle，縮寫：MAV) 此機型翼展長 0.5 公尺含以下，飛行距離最多為 2 公里。

(二)小型無人飛行載具 (小型無人飛行載具，Small-UAVs)

1. 目視較近距離無人飛行載具，可載重 5 公斤以下，飛較低高度及飛行在 5 公里範圍內。

2. 短距離的無人飛行載具，飛行的距離為 20 公里內。

大部分商用無人機為微型或是小型無人飛行載具。

(三)戰術型無人飛行載具至少具備 20 小時以上的飛行時間，且可依任務訂定時間，高度至少高達 18,000 呎左右。

二、無人飛行載具依其用途區分：

(一)軍事 (大型、長程、高飛行高度)

(二)商業 (中小型、短程、中飛行高度)

(三)休閒用途 (小型、低飛行高度)

三、依性能及用途區分：

無人飛行載具依其性能及用途可分為消費與工業級/專業級兩類，消費與工業級無人飛行載具，是針對家庭或個人用途設計的機型，通常裝有攝影及拍攝功能，大多是飛航拍攝玩家使用，其缺點是安全性較差、不穩定，常有失事情況及傷人的意外發生。

本研究是以微型及小型的無人機為論述重點，無人飛行載具依用途不同而具有各式各樣地外型與種類。目前在國外，無人飛行載具用途主要用於休閒娛樂及小型包裹運送等。現在許多國家都將它廣泛運用於國家水土保持監控、軍事情報偵察、緊急應變救災及太空探險等。

2.2 無人飛行載具闖入禁區

台灣民航法遙控無人機於 109 年 3 月 31 日上路，先前受爭議的【活動區域範圍】空域的圖資也一併更新，以紅色、黃色及綠色三種顏色標示禁飛區域(紅色區域)、限飛區域(黃色區域)及合法地活動的區域(綠色區域)。有別於之前超過全台一半縣市均顯示禁飛區域，更新後的圖資所標示的合法活動的區域(綠色區域)明顯增多，但部分縣市還是很多是禁飛區域(例如軍方軍事區域、機場等)[2]。

2.2.1 禁區定義

關於新版的空域圖資「紅色、黃色及綠色」三色代表的意義，民航局說明綠色區域代表合法地活動區域，無論是法人或自然人，必須遵守規定方可從事遙控器無人飛行載具的活動，法人另外可透過申請的方式申請活動許可，則可排除限制項目，申請許可則集會遊行、夜間飛行或噴灑相關物品。

紅色區域則屬於禁限航區域，機場或飛行場域及四周，與各縣市政府公告禁止區域，僅提供法人有通過審查鑑定後與飛航活動申請後，才能從事遙控無人飛行載具的活動。至於黃色區域是有條件的限制活動區域，主要區域為機場四周 60 米以上為禁航之範圍，與各縣市政府限制區域，自然人或法人操作者操作無人飛行載具時，限制

飛行高度為 60 米以下，法人必須申請活動許可，方可限制排除飛行，以飛行場域的經緯度座標為中心點，半徑 1KM 圓形區域為範圍，自水面或地面起為飛行場域四周禁止從事遙控無人飛行載具飛航活動的一定距離範圍內，如圖 2 所示，無人飛行載具空域圖資，列舉下列重點：

- 一、飛行高度綠色區域需在 120 米（四百呎）以下，黃色區域 60 米以下。
- 二、僅能於合法綠色區域及黃色區域飛行，不得在紅色區域飛行。
- 三、單人操作者最遠地飛行距離 300 米之內（以操作飛空者為圓心的半徑起算）。
- 四、必須離高速公路、鐵路、高架的鐵路、快速道（公）路、高架或者地面的捷運系統、障礙物及建築物 30 米以上。
- 五、僅能在白天時間飛行（白天定義為日出時間後，日落時間前）。
- 六、不得於室外集會遊行或人群聚集的上空區域活動；不可在移動中之船艦上或車輛操作遙控無人飛行載具；不得以遙控方式向無人飛行載具噴灑或投擲任何物件，亦不得裝載危險的物品。
- 七、一個人同一時間只能操作一台無人飛行載具；酒後不能操作無人飛行載具（血液中酒精的濃度必須小於 0.02%或吐氣時的酒精濃度必須小於每公升 0.1 毫克）。
- 八、無人飛行載具未達 2KG 不須操作證，250 公克以上無人飛行載具則需要註冊。
- 九、註冊號碼必需用標籤、噴漆、鐫刻或其他可以辨識的方式註明，確保每次進行飛行活動時不會掉落並且保持清潔、註冊號碼必須明顯且辨識。
- 十、註冊號碼的有效期限時間為二年，所有人必須於有效期限屆滿前三十日內，向民航局申請延展註冊號碼的有效期限；另台灣商港區域另有商港法規範無人飛行載具。
- 十一、軍事地區的敏感設施另設有要塞堡壘地帶法規範無人飛行載具；國家公園與河川管理地區另設有國家公園法或河川管理辦法規範無人機。

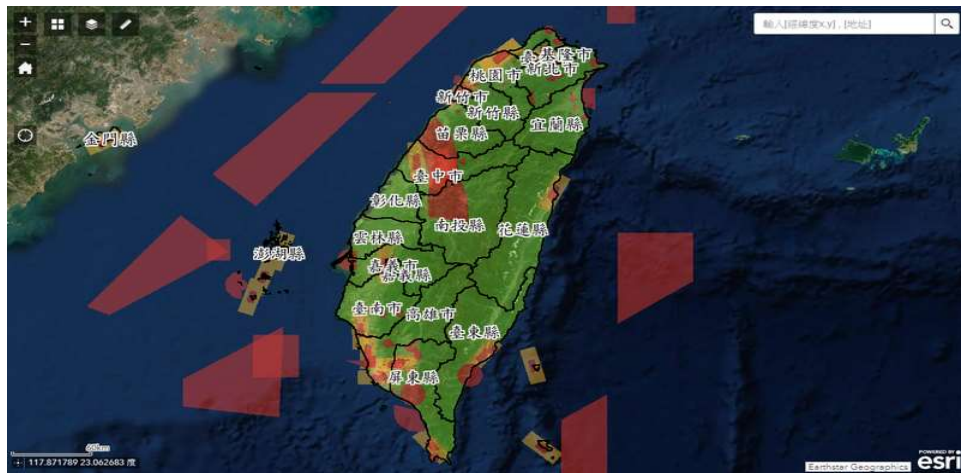


圖 2、無人飛行載具的空域圖資

(資料來源：文獻[2])

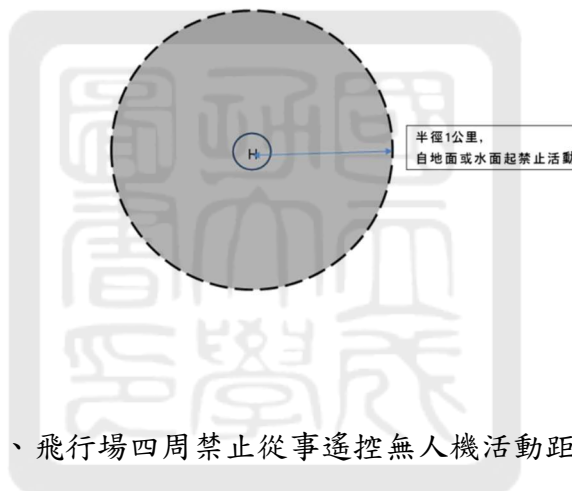


圖 3、飛行場四周禁止從事遙控無人機活動距離範圍

(資料來源：文獻[2])

交通部民用航空局的機場四周禁止施放有礙飛航安全實施要點中，此要點所稱有妨礙飛行(航)安全物體，是指人為施放之天燈、風箏、氣球、煙火(高空煙火)或可能影響航空載具的飛航安全之移動物體或漂浮（含無人飛行載具）等，如圖 3 所示，飛行場四周禁止活動距離範圍。

以機場跑道兩邊的中心點當作圓心，半徑五公里(KM)向外左右兩邊各 35 度所劃的弧形與以機場跑道中心線的左右兩側各 2.6(KM)地區域所匡列範圍以內，禁止施放有妨礙飛航安全的物體，如圖 4 所示，機場四周禁止施放飛航安全距離。

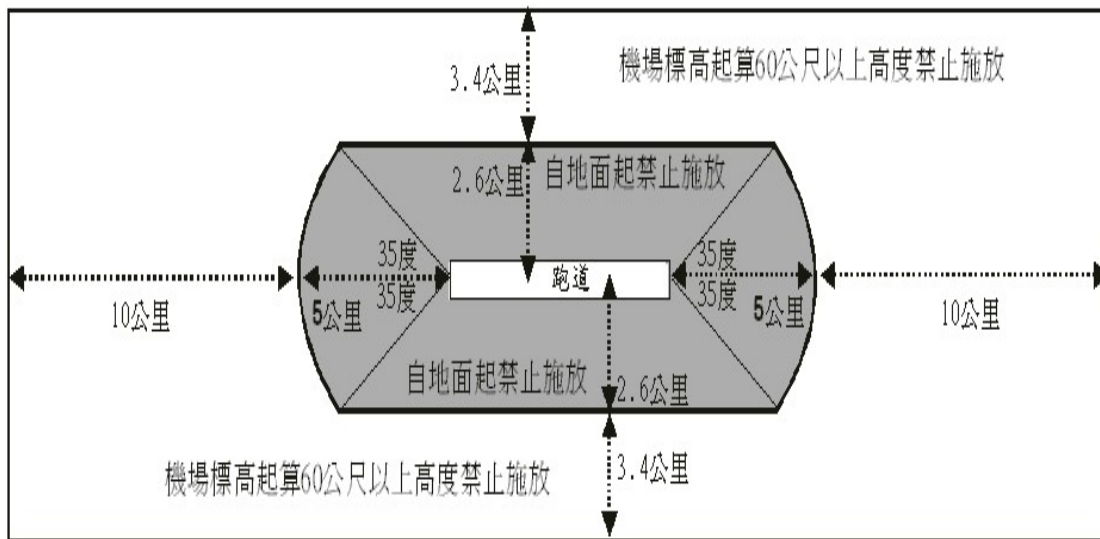


圖 4、機場四周禁止施放有妨礙飛航(行)安全距離範圍

(資料來源：文獻[2])

2.3 反制無人飛行載具

由於通訊導航技術及電子產業半導體的快速進步，無人飛行載具技術現今已廣泛應用於各領域，如空拍、測繪、農業及情資偵監等。雖然科技帶來相當的便利，卻也對於一般民眾的隱私或是飛航安全造成重大的影響，因此出現許多反制無人飛行載具的技術。雖然現階段國內、外已初步規範無人飛行載具的使用方式與規範，但對於無人載具的反制方式如何在機場及其周邊區域等關鍵區域卻無相關研究。現有反制無人飛行載具技術有區分軟體入侵方式及硬殺兩種，軟體入侵方式技術層面較高較為複雜，也對於周遭的影響最小，但是軟體入侵方式的技術多集中通訊監管、阻斷及干擾，尤其現代飛機航電及助導航設備所採用的電子、電氣系統設備大幅增加，相關設備的連接網路不僅種類繁多，無線頻段範圍也時常相互重疊，因此當軟體入侵方式在使用時也可能會有頻譜重疊的狀況發生，亦會造成飛航的安全[9][10]。

從技術層面來看，反制無人飛行載具系統的技術可分為監管型策略、干擾型策略與殺傷型策略分類。從無人機系統層面來看，大致可分為軟體入侵方式與硬殺傷方式兩類，「軟體入侵方式」是以電磁波或全球衛星導航的系統反射接收儀(Global

Navigation Satellite System-Reflectometry, GNSS-R)干擾敵方的頻率(包含無線頻段及 GPS)，而「硬殺方式」是直接對無人機進行摧毀。在實際運用中，則將常常會有兩種方式一併使用[11][12]。

軟體入侵方式是採取無線電技術手段使目標無人機非摧毀性失效、非破壞性(非摧毀)方法的應用常常希望能夠於可用情況下(盡可能)占有敵方無人機，甚至竊取其技術，最具代表性技術為無線電干擾及 GPS 干擾，使作戰目標中斷、入侵與更改全球定位系統等相關程序如下：

- 一、引導無人飛行載具到達目標的控制信號。
- 二、無人飛行載具向地面控制點回傳信號。
- 三、無人飛行載具位置參考信號(GPS、GLONASS 及 GALILEO)。
- 四、無人飛行載具獲得並發送給操作員/用戶的訊號。
- 五、駭入無人飛行載具系統軟體

2.3.1 反制無人飛行載具發展

於作戰需求與各方面的安全考量下，使得反制無人機的技術有基礎理論依據及高技術層面，也是因為各國遭受無人機攻擊後所延伸出反制無人機系統，因此從軍事用途為主的反制無人機的技術體系可分為以下三部分[13]。

2.3.2 反制無人飛行載具分類

反制無人飛行載具技術的體系有監管控制技术層面、干擾技術層面、摧毀技術層面，主要基於以下考慮因素：實施反制無人飛行載具作戰時，首先要對無人飛行載具進行探測技術及監控技術或干擾技術，再依據戰場地實際情況，選擇對無人飛行載具實施打擊的硬殺方式直接摧毀。

- 一、監管控制技术，藉由無人飛行載具的傳輸代碼控制無人飛行載具並引導其返航，且避免無人飛行載具直接墜毀。主要包括雷達監測跟蹤技術、地面的偵察技術與衛星的偵察技術等，並運用這些技術與地面偵察能力、雷達設備與衛星訊號組成

空中偵察系統，對無人飛行載具實現監測系統與預警系統，為後續的反制無人飛行載具作戰及偵察行動提供情報；如果下達控制指令上的偽裝欺騙訊號，則必須先知道無人機與遙控器的 ID 碼，再用軟體的先將掃描、使用軟體去破解鏈路(圖資情傳)編碼方式與加密方法等。

二、干擾技術主要包括控制信息干擾技術、數據鏈路(圖資傳輸系統)干擾技術及 GPS 定位干擾信號等三種方式，其中無人飛行載具發射無線電頻率干擾，以截斷無人機與遙控平台之間的通訊定向功率干擾射頻訊號，迫使無人飛行載具自行降落或返航；另一方面，絕大部分無人飛行載具的飛行控制系統均採用 GPS 與慣性導航系統互相結合，所以，干擾阻斷類的反無人機也可以干擾無人機的 GPS 信號接收機，導致無人飛行載具只能依靠本身陀螺儀的導航系統自行降落或返航。

三、摧毀技術主要包括反制無人飛行載具雷射武器技術、飛彈技術、微波武器技術及火力摧毀技術等，反制無人機最典型的反制機雷射炮。其實不只雷射砲，還有運用防空武器、彈射武器、榴霰彈武器及捕捉網等，這些技術的反制無人飛行載具武器裝備組成地面的防空火力，根據相關偵蒐提供的情報資訊，配合情資，運用戰術戰法，對無人飛行載具實施武力直接摧毀。

2.4 通訊的干擾類型

目前，對無人飛行載具的控制大多均使用無線電通訊的技術，對於目標無人飛行載具的飛行控制系統發射同頻段且較大功率的干擾信號，對於圖資下鏈信號則進行干擾及對於無人機的 GPS 定位系統進行干擾讓它自行降落或返航。

民間公司研究出反制無人機則是運用干擾槍就是利用這原理[14][15]。無人機干擾槍是運用電子(無線電)干擾系統，當扣扳機時，則干擾槍會向無人飛行載具發射全頻段(2.4G 或 5.8G)的干擾信號或衛星定位(GPS)干擾信號，使無人飛行載具脫離操作者的控制與衛星定位(GPS)信號，接收器接收不到控制信號或失去衛星定位(GPS)訊息，使無人機無法正常飛行，則無人飛行載具會依據衛星定位(GPS)信號設計不同會產生

降落、返航及墜落情形；一旦無人飛行載具的信號處於混亂的狀態，它通常有幾種選擇方式：先跌落到地面(通訊傳輸中斷無線電干擾)、返回操作者身邊(設定值設定 GPS 定位位置回操作者)或平穩下降(設定值回原廠設定 GPS 設定)。

2.4.1 無人飛行載具無線電通信頻段

Wi-Fi 的低功率射頻電機，必須依據 NCC(國家通訊傳播委員會)【低功率電波輻射性電機管理辦法】規定，且在辦法中【低功率射頻電機技術規範】並審認合格，則可使用 2.4 GHz 至 2.4835 GHz(簡稱 2.4G)，5.725 GHz 至 5.875 GHz(簡稱 5.8G) [16]。依據辦法中第 14 條規定，低功率射頻電機使用時不可影響飛航安全及干擾合法的通信；一旦有干擾情況時，則立即停用(止)，且必須改善到無干擾情況時方可繼續使用。

我國低功率電機技術規範規定的 2.4GHz 頻段(2400~2483.5MHz)，共有 CH1 (通道)(中心頻率為 2412MHz)到 CH13 (通道)(中心頻率為 2472MHz)等共計有 13 個(CH) 通道，每一個通道的中心頻率間隔都為 5MHz，因該頻段使用頻寬為 20MHz，在無人機設備的接收靈敏度為-75dBm 範圍內，只有 CH1、CH6 及 CH11 間有較少的鄰近頻率情況；2.4GHz 中心頻率為 2.45GHz，範圍為 2.412GHz~2.484GHz，分為 14 個波段，每個波段用的 20MHz 的無線載波的信道，每個信道之間的間隔為 5MHz，因此相鄰信道不是相互獨立，只有 3 組相互獨立頻道相鄰的多個信道存在頻率的重疊(如 1 通道、2、3、4 及 5 通道會有頻率的重疊)，如圖 5 所示。

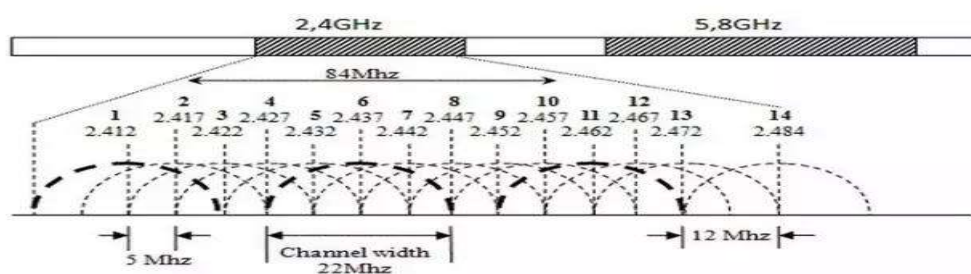


圖 5、2.4G 頻段碼框圖

(資料來源：文獻[17])

2.4.2 無線電通信展頻

無線電展頻技術最主要分為「跳頻技術」及「直接序列技術」的方式。當初是在無線電複雜的戰爭環境中，仍須保持通信信號保密性及穩定性所發展出來的技術。展頻技術在無線區域網路中的運用則是依 FCC(Federal Communications Committee；美國聯邦通訊委員會)規定的 ISM(Industrial Scientific, and Medical)，頻率的範圍在 902MHz~928MHz 及 2.4GHz~2.484GHz 兩個頻段間[17]。

一、跳頻技術(FHSS)

無線電的跳頻技術(Frequency-Hopping Spread Spectrum；FHSS)是在 2.4GHz 頻帶以 1MHz 頻寬將區分為 75~81 個無線電頻率通道(Radio Frequency Channel；RFC)，並在接收端與發送端兩端一樣的頻率用跳躍模式(Frequency Hopping)來接收或發送訊號以防止資料擷取。

二、直接序列展頻技術(DSSS)

在直接序列的展頻技術中(Direct Sequence Spread Spectrum；DSSS)將原”0”與”1”高功率及窄頻寬訊號，透過相位移轉技術(PSK；Phase Shift Keying)與虛擬隨機序列(PRS；Pseudo Random Sequence)，轉為低功率、寬頻帶(於 2.4GHz 頻帶，分為共 13 個通道，每個通道頻寬為 5MHz)的載波訊號，轉變後的載波訊號稱為 Spreading Chips。

三、跳頻技術與直接序列展頻技術調變差異

如果以單一頻寬來比較，由於展頻技術每個頻道在傳輸訊號時，所使用的頻寬(22 MHz)遠大於跳頻技術的頻寬(1 MHz)，一般而言，頻寬愈寬表示可承載的傳輸速率愈高，因此，展頻技術可獲得的資料傳輸速率大於跳頻技術展頻傳輸。大部分的跳頻技術都是使用高斯頻移鍵控(Gaussian Frequency Shift Keying GFSK)的調變方式。然而直接序列展頻技術則適用於對抗同頻干擾用可變相位調變 PSK、

QPSK(Quadrature Phase Shift Keying)及 DQPSK(Differential Quadrature Phase Shift Keying)等，得到最高可靠性及高數據速率。

2.4.3 GPS 原理

現今全球有四個國家的衛星定位系統，分別為美國的全球衛星定位系統(Global Positioning System, GPS)、俄羅斯的格洛納斯 (GLONASS) 系統、歐盟的伽利略 (Galileo) 系統及中國北斗導航系統。在這四個衛星定位系統中，美國全球衛星定位系統是目前世界上最常用的全球衛星導航定位系統，可供一般民眾使用的衛星導航定位系統。然而俄羅斯的格洛納斯系統，在我國僅有少數智慧型手機支援；中國的北斗導航系統；而伽利略系統則僅供歐盟國家使用。上述可見，目前供我國使用之衛星定位系統僅有美國的全球衛星定位系統，為無人機主要使用的衛星定位系統，此系統稱為「全球衛星定位系統」[18]。

全球衛星定位系統，由美國國防部負責研製與維護。由於全球衛星定位系統在全球的覆蓋率高達 98%，可提供高準確率的定位及檢測移動速度。全球衛星定位系統能夠順利運作，須由 3 個部分共同協力完成：分別為太空部分 (Space Segment)、地面控制系統 (Control Segment) 與使用者端系統 (User Segment)。目前，在正常情況下絕大多數消費者的無人飛行載具都會選擇全球衛星定位系統導航以控制無人機，而民用的全球衛星定位系統信號是無加密的，這就成為駭客入侵的機會。

GPS 欺騙原理則是向無人飛行載具的全球衛星定位系統發送假的地理位置(方位)坐標，進而控制無人機的導航系統，引誘無人機飛向所設定的地點。全球衛星定位系統可以由發送器所產生，亦可以是事先規劃錄製好然後讓無人機程序重放。因為無人飛行載具接收 GPS 信號是以(訊號最強)信號源為基準，因此在干擾欺騙的地面的 GPS 信號只要強度夠強大，亦可以覆蓋真正的從太空回傳來的 GPS 信號，進而欺騙無人飛行載具的 GPS 接收模組。通常無人飛行載具的操縱者與禁航區(紅區)之間有一定距離；無人飛行載具從操縱者附近地點起飛，然後逐漸飛往禁航區(紅色區域)。當無人

飛行載具到達禁航區(紅色區域)的附近，就能夠有效的偵查或破壞活動當下，此時無人飛行載具到禁航區的距離，通常比到操縱者(操作者)的距離還要近，然而地面的 GPS 會比無人機操作者訊號還要強。

目前，各國家都會在核心(重要)區域設置禁航區(紅色區域)，因此許多無人機的製造商在無人機內直接設定(出廠值)，在禁航區(紅色區域)內無人飛行載具無法起飛，即使到了禁航區(紅色區域)也會自動降落。因此，只要地面的 GPS 訊號將地理位置模擬成為禁航區(紅色區域)的定位(坐標)經緯度，就可迫使無人飛行載具自行降落。在 2015 年世界駭客大會上，其中有一公司的資安團隊表演了對無人飛行載具的全球衛星定位系統欺騙，成功地使正在飛行無人飛行載具降落地於面上。

2.4.4 GPS 干擾原理

從訊號程序的角度對應的反制無人飛行載具就會變成單純的訊號干擾情形、通過無線電及雷達方式將駭入系統的控制迴路與無人飛行載具飛行參數進行修改。從系統的角度來看，無人飛行載具在飛行控制迴路包括地面的飛行控制中心(發射端及接收端)，數據傳輸(圖傳系統)路徑與飛機本身。



圖 6、反制無人飛行載具的原理圖

(資料來源：本研究整理)

干擾的 RC(無線電頻段遙控器)向無人飛行載具發送的信號：干擾分析是先對遙控的發射器對到飛機訊號(控制的命令)攻擊(上行鏈路)。在如圖 6 所示，用字母《A》標示。假設無人飛行載具具有自行切換到自主模式功能，因此通常在失去了控制信號後，無人飛行載具會返回起飛位置並試著直接著陸，又或者無人飛行載具最後被引導到另一個位置，在從那裡重置並正確的連接。

干擾無人飛行載具向 RC(無線電頻段遙控器)發送信號：控制迴路的命令中斷，亦可能干擾所謂(下行鏈路)，在圖 6 中標示為《B》。在此情況下，無人飛行載具必須進行視覺或自行導航階段。

無人飛行載具則向飛行控制系統人員提供訊息干擾：一些無人飛行載具被用作為間諜方式，它們在飛行載具上獲取的信息則被發送到地面。

干擾無人飛行載具全球衛星定位系統參考信號：亦可能干擾的是全球定位系統訊號。假設干擾成功，若無人機則依 GPS 導航定位，無人機被迫只能著陸。重要的是要討論產生全球衛星定位系統的錯誤信號的可能造成「GPS 欺騙」。就是「偽衛星」的實現，如果無人飛行載具捕捉到一個錯誤信號，且在無人飛行載具上的 GPS 感測器將評估為「錯誤」訊號位置，那麼很有可能是指定無人飛行載具位置錯誤而導致相關任務失敗，進而達到自我防禦的效果。

在 2011 年 12 月 4 日，伊朗通過運用俄羅斯的車載電子戰系統，對裝置衛星數據鏈路加密程度非常高的美軍 RQ-170「哨兵」無人飛行載具成功實施控制引導，成功將其捕獲。通過無線電手段反制無人飛行載具技術已在戰場環境得到實戰檢驗，正因如此，各國與相關公司積極研發出更高端的電磁干擾技術以反制無人飛行載具系統[19]。

2.5 文獻歸納

目前全球反制無人飛行載具技術最主要是著重在監管技術、干擾鏈路技術與摧毀方式等 3 方面。監管技術最主要是於運用無線電或雷達感測器，將感應無人飛行載具入侵監控（技術層面最高）；干擾技術包括無線電頻段干擾、數據鏈路干擾及定位干

擾等，使無人飛行載具失去飛行控制系統及全球衛星定位系統；直接摧毀攔截科技著重於武器、雷射及捕捉等。無人飛行載具應用，對人類便利與科技是有幫助的，但無設定相關合法區與禁航區則會危害飛航安全；除以防禦設施(系統)於設置於重要場所(禁航區)外，更需要訂定嚴格使用方式與規範，以維持飛航安全，與本論文較相關文獻如下：

緣起：文獻[1][2][3]是針對為何做此研究的文獻參考，起源於戰爭中使用無人機攻擊行為與無人機入侵機場後影響飛航安全，蒐整國內外利用無人機的軍事活動、對社會民生物資的攻擊及對重要政經人員與關鍵設施威脅行為，無人機的威脅是全方位的，可用在軍事作戰上，也可用於攻擊重要政府高層官員，以及關鍵基礎設施，甚至用於攻擊平民，企圖影響另一國的政治、經濟穩定，製造社會動亂，以達到其政治目的。

規範：文獻[3][4][9][10][16]及[23]是無人飛行載具相關法的規範依據，針對無人飛行載具作詳實的介紹，及世界各國對於無人機如何管制，並介紹我國從無人機的型式、重量及體積區分，並規定操作無人機的操作者必須先行註冊登記無人機，也管制操作者必須擁有無人機執照，方能操作無人機。

原理：文獻[14][15][17][21]是以無人機的飛行與操控原理文獻，透過無線電的飛行控制原理，找出自由空間損耗及等效全向輻射功率的無線電原理與無人機的構連方式，並結合上述原理研究反制無人飛行載具之方法。

策略：文獻[6][12][13]無人飛行載具反制(防禦)系統管理評估研究，並針對無人機發展趨勢、研判無人飛行載具目前管制的問題及方式，再就目前無人載具反制(防禦)概念及反制(防禦)方式訂定三種策略方式，本研究就以此三種策略為論文研究方向。

第三章 研究方法

3.1 研究系統架構(監控管制類型)

所有無人機都運用無線電的手段遙控、圖像傳輸及衛星定位，而有些無人飛行載具則可以採用如圖像識別、地形樣貌對照及高精度導航的方法來確定本身位置，且能自主完成任務。既然無人機必須使用到無線電技術，因此可以對無線電頻段實施干擾，而使無人飛行載具失控落地或折返的目的地。

監控管制類型反制無人飛行載具對技術層面的要求最為複雜，不要求不可損傷(害)無人機本身的前提下並完成對無人機控制信號的阻斷情形，需要使用控制指令偽裝、欺騙及軟體掃描入侵。

3.1.1 理論依據(無人飛行載具控制器配對)

無人機遙控端 2.4G 射頻有分為發射模組及接收模組，開機後就會啟動自動掃頻功能，會有 50 個以上工作通道。每一個遙控器會對應配置一個接收機。遙控器(發射機)及接收機需要配對使用，如圖 7 所示，無人飛行載具遙控訊號的構連圖，不同廠商則無法相容配對，因為使用的收發芯片與協議可能會不一樣。每一台遙控器(發射機)都匹配一個固定的 ID 碼框[20]。配對接收機時則先讀入發射機的 ID 碼(對頻操作使用)。假設此接收機中途與其他發射機進行配對，則下次再使用遙控器(發射機)時，仍需與遙控器(發射機)重新進行對頻(比對)操作。每個遙控器都有一組唯一的 ID 碼。因此所有的無人機遙控器都先必須進行配對 ID 碼才可和無人機(接收機端)構連，若因無法與無人機配對 ID 碼時則無法控制無人機，而且配對的流程一定是開機後再進行配對流程，所以無法在無人機的飛行過程中去監測 ID 配對碼，亦不可能在飛行過程中搶奪控制權，僅能當無人飛行載具失效或落地後，以軟體無線電(Software Defined Radio, SDR)方式去配對 ID 配對碼，而建立遙控器(無線射頻訊號)與無人機的通信訊號，此時開啟遙控器(無線射頻訊號)及無人機會自動完成配對，首次對碼信息僅僅由遙控器發出，無人機僅接收這個信息，但是對於監管控制的

方法我們需要去模擬獲取到無人機的控制權及無人機與遙控器的一次對碼信息，因此無法在第一次直接監管遙控器(接收機端)，所以必須先讓無人飛行載具失效後方能監管。



圖 7、無人飛行載具遙控訊號構連圖

(資料來源：本研究整理)

3.1.2 理論依據(遙控器信號解譯)

遙控器大多已改為展頻及跳頻方式的數位遙控器，發射頻率為 2.4GHz，要複製此遙控信號且以較強的發射功率進行干擾或蓋台方式比較容易，著重點在於探討困難度較高的數位遙控信號複製技術。目前 2.4GHz 頻段的數位遙控信號是分碼多工(Code Division Multiple Access, CDMA)連接技術為主，可分為直接序列展頻及跳頻展頻，包含兩者的混合使用；分碼多工的展頻技術可讓多個遙控器共用，當使用相同頻段不會互相干擾情況，且在有障礙物遮蔽的多重路徑環境下，傳輸穩定度仍有良好的表現。

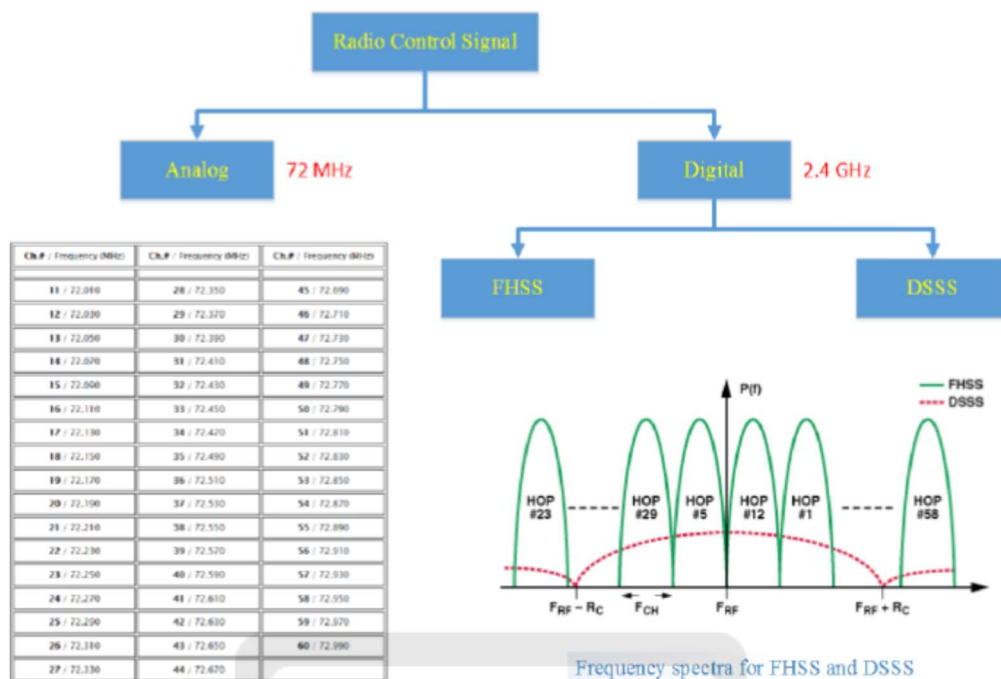


圖 8、直接序列展頻與跳頻展頻

(資料來源：文獻[17])

直接序列展頻：直接序列展頻技術是較可靠的無線電鏈路連結，基本原理是將發送基頻(Base Band)訊號轉換能量變低，但再使用展頻 (Spreading Signal)訊號傳輸出去，可同時將直接序列展頻的技術提高對於環境抗干擾的能力增加；如圖 8 所示，直接序列展頻是將原始訊號是透過兩次展頻方式處理，可獲得還原訊號；因此在第一次展開的訊號中大氣環境傳播過程中，可能會和環境的干擾訊號一起被無人機端所接收，因為這些訊號必須經過處理，於是原始訊號還是被還原了，同時雜訊(干擾源)也會被直接展頻碼會變成低功率高頻寬的訊號，這樣的方法就是利用濾波器將雜訊與原始訊號分離 (區分)，所以，就可以對抗環境所產生的干擾源。

跳頻展頻：跳頻展頻是一種展頻模組結構方式，使用窄頻會以發送端及接收端同樣的協定方式變更頻率。經過適當的同步處理後，兩個裝置(發送端及接收端)就會維持單一邏輯通道。對非目標接收器來說，跳頻展頻就像是短脈衝雜訊。更簡單地說，

資料則會分解成封包形式，由多個「跳頻」（共 79 個）以虛擬亂數的方式，將封包傳輸至接收端。只有在同一跳頻模式上同步的發送端及接收端，才能存取傳輸資料。發送端每秒會切換跳頻達 1,600 次，確保資料維持高度安全性。

3.1.3 理論依據(無線加解密)

高級加密標準 (AES) 於 2001 年 11 月 26 日由美國國家標準與技術研究院 (NIST) 發佈為 FIPS PUB 197，自 2002 年 5 月 26 日起成為密碼學標準；主要由四個步驟組成，SubBytes、ShiftRows、MixColumns 和 AddRoundKey，密鑰大小為 128 位元、192 位元或 256 位元，取決於所需的安全級別。

AES 演算法共有三個重要的參數：

- 一、加解密區塊數量：加密與解密的訊息，以 32 位元為一單位。
- 二、金鑰區塊數量：金鑰的長度，以 32 位元為一單位。
- 三、運算回合總次數：加密與解密編解碼運算的回合總次數。

在依 AES 標準規範，可分為：AES-128 位元、AES-192 位元及 AES-256 位元，然而在 AES 加密過程中，相同的操作重複 10 次，12 次或 14 次（也稱為總回合數）。賦予該算法的密鑰被擴展成長度為 4 byte 的 44、52 或 60 個字組。AES 的加密，首先將明文區塊與第 0 回合金鑰 RK0 進行 XOR 運算，以產生相應的密文塊，稱為狀態矩陣，接著循序做多次的回合運算；另外 AES-128 位元、AES-192 位元及 AES-256 位元的意義是指， 2^{128} 、 2^{192} 及 2^{256} 種可能，如果要用 256 位元（總計 78 位數字）必須以超級電腦去運算，而且還要花上萬年才可運算完成（解密），現今有量子電腦運用量子理論（針對加密演算法運算）與機器學習（針對數學運算）結合，達到量子加速運算的優勢，但量子電腦需要大量的運算與高階的中央處理器，較無法從環境中建置。

3.2 研究系統架構(無線干擾類型)

目前，商業使用的無人飛行載具均使用跳頻、展頻技術及加密技術（比較少），且跳頻參數可以自行設定，並具抗干擾的能力。所以在計算干擾的功率時，必須先知道

跳頻、展頻的相關數據才能得到較準確的結果。但我們還是可以用干擾頻段範圍。遙控型無人飛行載具仍以相關頻段去干擾，但無線電的干擾功率就會比 GPS 簡單。但在干擾的同時，如果是較大的干擾功率則會影響其它正在運作的無線電通信訊號，因此必須去計算相關無線電射頻自由空間、接收機的靈敏度及等效全向輻射功率。其中以下就區分無線電干擾策略及 GPS 干擾策略兩部分。

3.2.1 理論依據(無線電干擾射頻自由空間)

無人飛行載具的無線電飛行控制回傳，電磁的干擾槍算是現今最常看見的無人飛行載具的反制設備，是在非法區域內對無人機發射無線電射頻頻段及導航信號頻段（2.4GHz 的，5.8GHz 的，GPS 的 L1 及 L2 等）電磁波干擾，以干擾無人機的遙控鏈路通訊系統及 GPS 導航，使通訊、導航系統失靈，迫使無人機在空中懸停、返航或是降落地面[21]。

無線電在自由空間中傳播，先不論是否遭遇障礙物遮蔽或是反射及折射問題，都會因為傳播距離造成傳輸衰減，本章節介紹在自由空間傳播時複雜的通信距離計算：而自由空間傳播是假設天線周圍為無限大真空電磁波傳播，假設在這個環境是理想傳播條件，因此電波在傳播時，能量既不會被障礙物所吸收，也不會產生反射也不會散射。這些都是在理想狀況的傳輸距離，如果我們在實際上應用一定是數值較低(因為會有反射及折射產生，會導致傳輸距離會變短)，是因為無線電通信會受到各種外界因素(例如地形、地物)的影響會造成損耗，如果將上述相關損耗參考值計算入式中，即可計算出相近的通信距離。

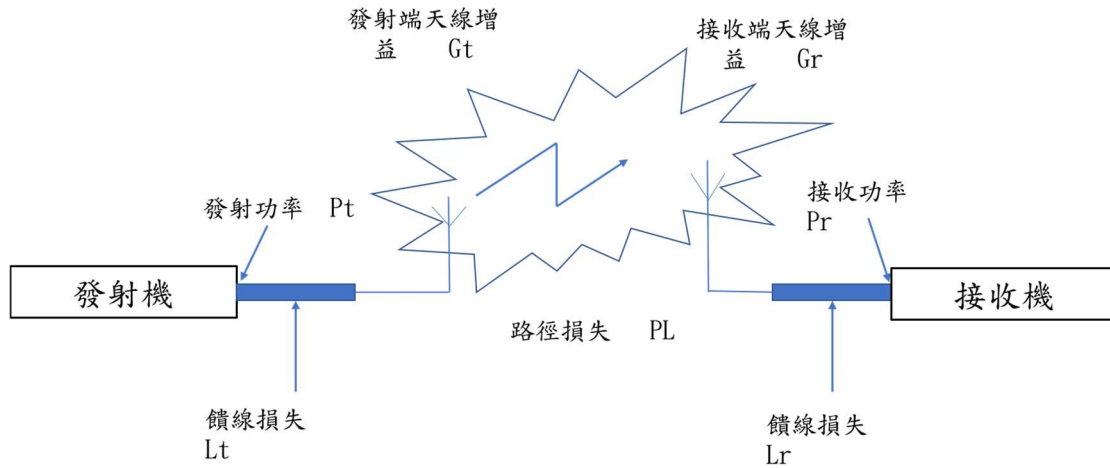


圖 9、無線通訊鏈路

(資料來源：文獻[22])

通訊系統間是否會引起干擾，其因素相當多，也是一個相當複雜的問題。可將此問題區分為發射端及接收端，及干擾源及被干擾源，如圖 9 所示，為一個典型的無線通訊系統之傳輸鏈路。在自由空間(Free Space)的傳播環境下，接收機所收到的功率 P_r 如下：

$$P_r = \frac{P_t \cdot G_r \cdot G_t}{L_t \cdot PL \cdot L_r} \quad (1)$$

其中上述公式， P_t 為發射功率， G_r 及 G_t 分別為接收天線增益及發射天線增益， L_r 及 L_t 為接收端天線饋線損失及發射端天線饋線損失， PL 為路徑損失。

本論文將假設無論接收端的饋線損失(L_r)與發射端的饋線損失(L_t)非常小，可假設饋線無耗損，饋線耗損率為 1，因此方程式(1)改寫如下：

$$P_r = \frac{P_t \times G_t \times G_r}{PL} \quad (2)$$

自由空間損耗描述了電磁波在空氣中傳播時候的能量損耗，電磁波在穿透任何介質的時候都會有損耗。根據國際電信聯盟無線電通信部門 (ITU Radiocommunication Sector，縮寫 ITU-R) ITU-R [23] 文件，傳播路徑損耗 PL 為

$$PL \text{ (dB)} = 32.44 + 20 \log d(\text{Km}) + 20 \log f(\text{MHz}) \quad (3)$$

上式中 PL 為傳輸的損耗單位 db ； d 為傳輸距離，單位為 Km (公里)； f 為頻率，其單位為 MHz 。一般而言，電磁波的頻率與波長關係為 $c=f \cdot \lambda$ ，其中 c 為光速。

另一方面，發射端所發射之電波訊號，傳播到接收機天線端處之電場強度，是評估是否會導致接收機受干擾之重要參數。這部分及發射之頻率、頻寬、電功率、天線、距離、發射型態等因素有關。特別是發射機及接收機間之距離，所以就是因為發射機及接收機(無人飛行載具)距離較遠，容易以較近的距離去干擾無人飛行載具(進入禁區時)，以干擾槍或干擾頻段讓無人飛行載具遙控失效或 GPS 失效，當距離越遠，則路徑中間的傳播環境，對訊號的衰減影響最大，所以是評估通訊系統之干擾重要因素；通信距離及發射功率、接收的靈敏度及工作頻率有關。

由上式可知，在自由空間的電波傳播(也可稱衰減)，只和發射頻率與傳輸距離有關，當頻率或傳輸距離增大一倍時，傳輸的損耗也會增加 $6dB$ 。

接收機三階截斷點把它定義為截斷點(Intercept Point, IP) [24]。如圖 10 所示，圖中的 IP_3 為三階截斷點(3rd-order Intercept Point, IP_3)。當輸入功率增加時，輸出基頻與 3 倍頻也會增加，輸入功率如果增加 $1dB$ ，基頻輸出也會增加 $1dB$ ，然而 3 倍頻輸出則增加到 $3dB$ ，是屬於線性區域。若輸入功率如果再繼續增加，最後則兩個都進入飽和狀態。

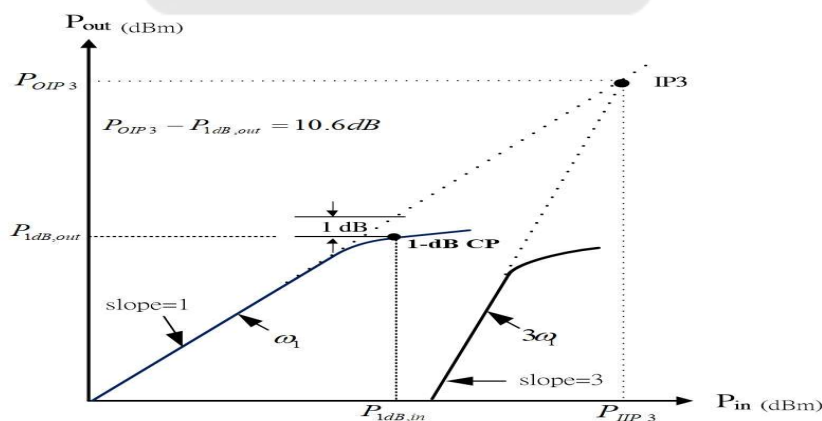


圖 10、 IP_3 是三階截斷點

(資料來源：文獻[24])

定義 2.4GHz 與 5.8GHz 之間的選擇也不難理解是屬於 802.11a：2.4GHz 可以提供較大距離，但信號較弱；而 5.8GHz 可以提供較強信號，但距離較短。802.11a 2.4G、802.11g 5.8G 頻段及 GPS 1.5G 頻段時各個 Pin(dBm)，如表 1 所示。

表 1、802.11a/b/g 接收器前端規範

	802.11a	802.11b	802.11g
Input Return Loss(dB)	>10		
Gain(dB)	20	20	20
NF(dB)	≤ 10 dB	≤ 10.5 dB	≤ 10 dB
IIP3(dBm)	≥ -20 dBm	≥ -10.3 dBm	≥ -10.3 dBm
IIP2(dBm)	≥ -3.2 dBm	≥ 17.5 dBm	≥ 17.5 dBm
Input Pin, max(dBm)	≥ -30 dBm	≥ -10 dBm	≥ -20 dBm

(資料來源：文獻[25])

IEEE 802.11a/b/g 規範，計算出符合 2.4/ 5.7 GHz，WLAN 規範的射頻接收機鏈路，在 IEEE 802.11a 中， $NF \leq 10$ dB， $IIP3 \geq -20$ dBm， $IIP2 \geq -3.2$ dBm， $Pin, max \geq -30$ dBm；在 IEEE 802.11b 中， $NF \leq 10.5$ dB， $IIP3 \geq -10.3$ dBm， $IIP2 \geq 17.5$ dBm， $Pin, max \geq -10$ dBm；在 IEEE 802.11g 中， $NF \leq 10$ dB， $IIP3 \geq -10.3$ dBm， $IIP2 \geq 17.5$ dBm， $Pin, max \geq -20$ dBm，以上述整理圖呈現。

3.2.2 理論依據(無線電射頻等效全向性輻射功率)

通訊干擾的產生，可以定義為接收端收到一定強度且不必要的訊號(目前本文的干擾情況)，導致其接收產生問題，如通訊中斷、通話品質下降、數據傳輸錯誤率提高等。一般而言，這及接收機的靈敏度，動態範圍，EIRP(Effective Isotropic Radiated Power)，調變方式等特性有關。因此，接收機的性能也會影響受干擾程度 EIRP(Effective Isotropic Radiated Power)為有效全向性輻射功率，也稱為等效全

向輻射功率，把衛星與地球上發射天線在波束中心軸向上輻射的功率稱為發送端的有效全向性輻射功率（EIRP），即為無線電發射機給天線的功率（ P_t ）與天線的絕對增益（ G_t ）乘積，為代表地球上發射或轉發器發射能力的重要指標。

各方向具有相同增益單位的理想全向天線，作為無線通信系統參考的天線。EIRP 定義為： $EIRP = P_t \cdot G_t$ ，其中 P_t 為發射功率， G_t 分別為發射天線增益。

因此依據方程式(2)發射機所需發射的等效全向性輻射功率

$$EIRP = P_t \cdot G_t = \frac{P_r \cdot PL}{G_r} \quad (4)$$

此為線性函數，所以當上式算式取對數之後

$$EIRP = P_t + PL - G_r \quad (5)$$

其中上述公式 P_t 代表發射機的發射功率， PL 為路徑損失， G_r 代表接受端天線的天線增益，設定上述為方程式(5)。

電磁波經由發射天線輻射後，經一段距離的傳播後，訊號強度會隨距離增加，產生衰落(fading)現象，如圖 11 所示，衰落程度愈大，愈不利接收，也意味著整體訊號強度變小，對其他通訊系統的影響較小。這些衰落現象又可分成路徑損失(path loss)、遮蔽(shadowing)效應、快速衰落(fast fading)。路徑損失指的是由距離引起的訊號衰減；遮蔽效應通常是由牆壁及建築物等形成之阻擋效應；快速衰落指的是由多重路徑引起的訊號衰減[26]。

電波傳播之衰減程度，受到路徑環境影響很大。例如，自由空間(free space)環境之傳播，衰落程度最小，只與距離有關。若在都會環境中，因大樓林立，且建築物之材質及密度較為複雜，就會有遮蔽效應及快速衰落現象，訊號的衰落會更為嚴重。

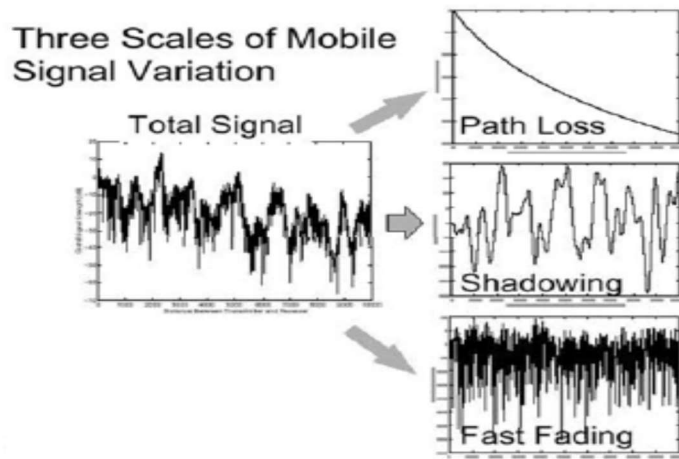


圖 11、無線通訊環境電波訊號

(資料來源：文獻[26])

3.2.3 理論依據(干擾阻斷 GPS 類型)

訊號是由載波、電碼以及導航訊息所組成的，解算此訊號可得到使用者之載體位置、速度等資訊。在生活上有非常管範的應用性，如：車用導航、地質測量、海洋運輸、智慧型手機中 APP 軟體的應用等。但當將數個電子模組或是裝備互相搭配使用，模組間相互干擾的問題便隨之而來，一旦產生干擾時，全球衛星定位系統(GPS)模組接收到的定位訊號就會變的不穩，使得 GPS 模組無法定位。

使用發射在太空中的 24 顆衛星再與地面上的監控站及用戶端設備的衛星接收器，以上述三個方位就能迅速地確定用戶端在地球上所處的位置(方位、座標)及海拔高度等。

目前世界上除了美國 GPS 以外，還有俄國、歐盟與中國的北斗衛星等四種衛星可利用，GNSS 則指所有衛星導航系統，如表 2 所示，全球所有衛星數量。

美國 GPS 的 L1 頻率大概為 1575.42MHz、L2 為 1227.7MHz，因為衛星廣播導航信號會產生延遲，進而產生誤差。而其對不同頻率信號所產生的影響不一樣，因此當接收雙頻信號後則可計算出並消除電離層的誤差。

表 2、全球所有衛星數量

衛 星 系 統	衛 星 數 量	使 用 範 圍
美國 GPS	24 顆	全球
俄國 Glonass	24 顆	全球
歐盟 Galileo	目前 4 顆	全球
中國北斗 BDS	目前 31 顆	2020 年全球 35 顆

(資料來源：本研究整理)

全球衛星定位系統(GPS)工作原理是接收機(無人飛行載具)，另一台或幾台接收機置於載具(以下以流動站代替)上，(無人飛行載具)與流動站同時間接收同樣的 GPS 信號，(無人飛行載具)測量的載波相位觀測數值、偽距觀測數值、(無人飛行載具)的坐標等，運用無線電波傳送資訊給流動站台，而流動站台透過無線電接收(無人飛行載具)所發射的訊息，將載波相位觀測數值進行處理，得到(無人飛行載具)與流動站台的向量 (ΔX , ΔY , ΔZ)。

在衛星定位測量數據處理過程中，主要任務是求基線向量。因此它的計算程序是：利用三差求出近似的基線長度，再使用浮動雙差法去求解出相位模糊度及基線量。求得的相位模糊度湊整後，再進行固定雙差的計算，最後求出精密的基線向量。

讓無人飛行載具認為是干擾的 GPS 給予的 GPS 訊號且在禁航區(紅色區域)所產生的 GPS 訊號較原訊號強，則容易產生受到干擾，有時候會在物體之間相互反射，這就意味著要更長的時間才能到達接收機；因此 GPS 也不是那麼完美的精準，水平方向的典型精度通常是 5~10 米。垂直方向大概是 15 米，GPS 最有用的方面就是它能夠給出無人飛行載具相對於地球的三維位置絕對值，再結合其他傳感器，如氣壓計測得的相對高度，將所有這些數據綜合起來，就能夠估算出無人飛行載具較為精準的位置。如果能連接到更多的衛星，也會使得估算的位置更加精準。

3.2.4 無人飛行載具干擾槍

無人機干擾槍是目前最常見的無人機反制設備，它的原理是於發射處發射無人飛行載具數據鏈路通訊及導航訊號頻段（2.4GHz 的，5.8GHz 的，GPS，BDL1，BDL2 等）電磁干擾波，以干擾無人飛行載具的飛行控制系統(遙控器)及導航電子系統，使其通訊鏈路收干擾、導航系統重新定位，以致產生返航、空中懸停或降落地面。

電磁干擾槍有兩大優勢為成本低及易攜帶；現今無人飛行載具干擾槍均為普通頻段、高頻段及導航干擾，則成本會高一點，如果有其他硬體設備成本也會提升。在攜帶方便而言，低功率的電磁波干擾槍體積較小，重量較輕，可隨身攜帶，機動性較高。但功率較高的電磁波干擾槍，體積與重量相對較大(機動性就不高)，但可固定於巡邏車上。

但電磁干擾槍也有三大缺點：不具監管功能，有輻射及射程距離較短。首先無人飛行載具干擾槍不具備無人飛行載具監測(監管)功能的，無法第一時間入侵無人機。另外就是電磁波干擾槍就是使用電磁波干擾就會有輻射的問題。理論上來講，發射功率愈大，射程則愈遠，同時輻射同時也愈大，如圖 12 所示，相關規格資料，如表 3 所示，本研究也是將此干擾槍規格去計算各頻段干擾時的距離，當做為未來干擾槍的設計依據與標準[27]。



圖 12、無人飛行載具干擾槍

(資料來源：文獻[27])

表 3、無人飛行載具干擾槍規格

型號	RAYSUM MD-1S
主體尺寸	66cm×24cm×28cm
主體含槍托	86cm×24cm×28cm
重量	含電力系統整套小於 6 公斤
使用電壓	DC 24V
使用溫度	10 度~55 度
使用時間	60 分鐘以上
充電時間	約 4 小時
頻率	2.4G~2.5GHz(飛行遙控器) 5.7G~5.9GHz(影像回傳) 1567~1620GHz(GPS 定位)
輻射功率	2.4GH/20W：58dB=630.9W 5.8GH/3W：42dB=15.8W 1.5GH/20W：49.9dB=97W
信號模式	DSSS(展頻)、FHSS(跳頻)
天線增益	定向天線 10~12dB
水平波束角度	40(±5)度
垂直波束角度	35(±3)度
有效干擾距離	1000 公尺

(資料來源：文獻[27])

3.3 反制無人飛行載具(摧毀類型評估)

近年來無人飛行載具威脅日漸增加，不僅在作戰時，無人飛行載具被軍事用途執行任務，然而敵對的國家、或非國家角色例如恐怖分子、叛軍或游擊兵，還是以無人飛行載具攻擊對方的政治、經濟及軍事設施等，甚至造成大量破壞及損失（例如油池等）；沙烏地阿拉伯表示，南部的石油設施在遭到飛行物體攻擊，儲油槽發生火災。在平時，無人飛行載具對重要政經人員和關鍵的基礎建設進行擾亂甚至攻擊，不但會影響公共服務的正常運作，更威脅到政府高層人員的安全，嚴重會造成重大經濟財務損失。這些用為攻擊手段的無人飛行載具，有些是屬於中大型機型，但更多的是便宜迷你小型的商用機型，甚至用簡單零組件即可組裝完成，要防範不易。無人飛行載具在軍事上的運用，已成為一種新的不對稱威脅作戰。

摧毀可說是最直接，粗暴且簡單的方法。如果不從技術角度區分。實際來講，主要是運用精準定位技術與監視系統，透過像光學或飛彈的方式直接攻擊無人飛行載具，此類型最簡單且粗暴方式即是摧毀目標，適用於不易干擾的環境，或是環境中無法容許無人飛行載具侵入的地點(如機場)。但系統價格相對昂貴，較重於軍事用途。

3.3.1 理論依據

摧毀技術包括反火箭、砲彈與迫擊砲系統、雷射及榴霰彈武器精準打擊及捕捉網型等反制無人機技術，運用這些技術的反制無人飛行載具武器，依據相關偵察的情報系統提供的情報訊息，運用合理的戰術戰法，對無人飛行載具實施火力摧毀。

- 反火箭、砲彈與迫擊砲系統，但成本較高的砲彈與防空導彈是防空武器系統，也是最常用的反無人飛行載具武器，其優點是技術成熟度高，不足是高炮攔截命中率較低、導彈攔截成本高，且不適合抵禦大編隊無人飛行載具群。
- 雷射及榴霰彈武器精準打擊無人機，功率有待提高鐳射武器通過對目標施加能量來破壞或摧毀目標。
- 捕捉網不損傷無人飛行載具，無人飛行載具槍，它利用壓縮空氣向來襲無人機

發射捕捉器，捕捉器在抵達無人機前爆炸，撒開捕獲網，將無人機纏住，由降落傘載著無人機降落地面。槍的作用距離為 100 米以內。



第四章 研究結果

4.1 反制無人飛行載具監管策略

很多國家對機場，軍事管理區等安全區域設置了禁止無人飛行載具進入的禁飛區，但是仍然可以看到很多因為非法無人飛行載具導致的民用航班延誤的問題。主要原因不是監管不嚴，而是對無人飛行載具的監管比較困難，松山機場因無人飛行載具違規飛行而導致機場關閉的狀況，往往影響航班時程與旅客行程。難以查獲施放者的主因為：飛行員從空中通知地面塔臺管制人員的範圍太大，且小型無人飛行載具均在三度空間竄飛，實難用定位的方式查察相關位置，員警趕赴可能地點時經常查無所獲(機動性太高)。

為保障航空飛行載具進場、離場及重飛場面的淨空，應提供安全的操作區域(空間)，以維護飛航安全，在民用機場或軍民合用機場四周的範圍內，施放氣球、煙火、天燈、風箏與其他可能影響航空載具飛航安全之漂浮或移動物體等，有妨礙航空飛行載具飛航作業之虞，應依相關規定向交通部民用航空局申請；經評估未影響飛安情況下，且機場無航空載具活動時，交通部民用航空局得核准方可放行，因此交通部民用航空局則立法規範無人飛行載具均需註冊使用及設置禁航區。

4.1.1 監管策略(無線遙控配對)

要先行以軟體入侵方式將無人飛行載具直接監管使用還是因為無人飛行載具的遙控器要先行配對程序 ID 碼，如圖 13 所示，故無法直接接管無人飛行載具，因為無人飛行載具的開機後的程序首要為配對遙控器(除非先前已先配對成功)，故只能於將無人飛行載具失效或落地後再進行，遙控器的配對接管與頻率操控，且要透過相關的頻段配對與熟悉各家廠商的資訊，才能運用入侵方式去接管無人飛行載具。



圖 13、遙控器與無人飛行載具配對圖

(資料來源：本研究整理)

4.1.2 監管策略(無線解密困境)

AES 利用區塊加密法(Block cipher)將明文分成多個區塊，每個區塊為 32 位元，區塊長度固定為 128 位元，並使用對稱金鑰對每個區塊分別加密，其金鑰長度則可以是 128 位元、192 位元或 256 位元。雖然金鑰長度越長能提供較高的安全性，但也會使運算回合次數增加，並且用 128 位元（16 位元組）分組加密及解密資料。

使用窮法破解金鑰關鍵長度在 192 位元以上的資料是不真實的。統計顯示，即使使用當前世界上運算速度的計算機，窮盡 192 位元金鑰關鍵還要花上數十年的時間，更不用說去破解採用 256 位元密鑰長度的 AES 演算法。

4.2 反制無人飛行載具干擾策略

干擾控制訊號是指干擾無人飛行載具與操作者的遙控訊號，相關流程圖，如圖 14 所示。

步驟一：在禁航區發現非法無人機，先以干擾槍干擾遙控信號，對於遙控器無線訊號干擾。

步驟二：如果無人機進入 GPS 導航階段，則以 GPS 導航訊號欺騙落地、懸停或返回。

因無人飛行載具在研發過程中，為了加強使用者控制訊號的強度，遙控接收天線的主瓣通常會朝向地面，這設計架構雖然加強對無人飛行載具的控制度，但也為反制無人飛行載具無線電干擾系統提供機會。雖然現在無人飛行載具遙控發射機普遍採用跳頻與擴頻技術，也必須設定在一定範圍內。簡單而言，只要判斷控制訊號的大概範圍多少，用聲音雜訊覆寫該頻段範圍，就可精準打擊無人飛行載具，達到反制效果。

干擾阻斷類型的反制無人飛行載具系統地應用較為廣泛的意義為針對目標無人飛行載具發射定向的大功率射頻頻段干擾，切斷無人飛行載具與遙控器之間的通訊，從而迫使無人飛行載具自行降落或返航。另一方面而言，由於絕大部分無人飛行載具的飛行控制均採用 GPS 衛星導航系統與慣性導航系統相結合的方式。

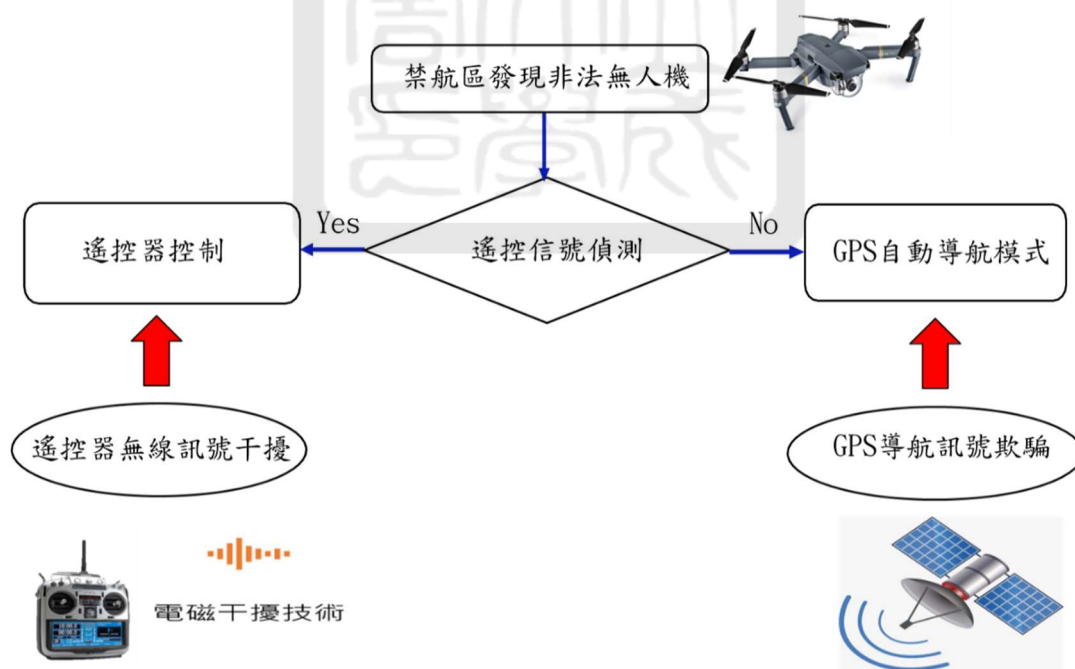


圖 14、無人飛行載具干擾欺騙策略圖

(資料來源：本研究整理)

4.2.1 反制無人飛行載具無線電阻斷策略(自由空間)

無人飛行載具對電磁干擾非常敏感，高功率微波、電磁脈衝都能夠使無防護的無人飛行載具電子元件會暫時失效或導致半導體元件直接燒毀，可讓無人飛行載具中運算功能損毀，從而使無人飛行載具陷於癱瘓甚至墜機，如圖 15 所示。因此，干擾阻斷策略的反制無人飛行載具系統在技術上較為容易實現。但隨著技術的發展，無人飛行載具抗干擾能力在技術層面越來越強大，在更多時候，普通的干擾阻斷頂多能讓無人飛行載具作業失敗，且對於被干擾後的無人飛行載具如何採取下一步較難推斷，難以達到防範預期。



圖 15、無人飛行載具無線飛控干擾圖示

(資料來源：本研究整理)

依據第三方程式計算，計算出在自由空間下的無線電環境計算出以距離間隔及禁區的規範下應該由防禦者(干擾)發出多少功率，藉由此方法去干擾無人飛行載具的飛行控制系統。

此為理想狀況的傳輸距離，實際的應用則會低於該數值，這是因為無線通信要受到各種外界因素的影響，如大氣(如霧霾等)、阻擋物(地形)、多路徑等造成的損耗。

再把方程式(2)與方程式(3)整理 $P_t = P_r - G_t - G_r + PL$

先以 0.5 公里(500 公尺)為計算範圍，頻率為 2400MHz，則可計算出

$$P_t = P_r - G_t - G_r + PL(32.44 - 6.02 + 67.60)$$

$P_t = -30 - 3 - 3 + (94.02) = 58.02(\text{dBm}) = 633\text{W}(500 \text{ 公尺})$ ； P_t 為干擾槍的發射功率大約為 58.02 dBm 約為 633W。

如果當距離為 1Km 時，則 $P_t = 64.04(\text{dBm}) = 2.5\text{KW}(1\text{Km})$ 。

如果當距離為 2Km 時，則 $P_t = 70.02(\text{dBm}) = 10\text{KW}(2\text{Km})$ 。

如果當距離為 3Km 時，則 $P_t = 73.58(\text{dBm}) = 22\text{KW}(3\text{Km})$ 。

對於禁航區無人機機動式干擾槍先干擾 2.4G 遙控器，但因為干擾槍的機動性要高無法太大功率，以上述的功率來計算大於 1KM(為 2.5KW)已經很大了，因此要防止禁航區的無人機因禁航區依相關規範為以塔台或機場中線為主向北或南延伸大約 1.5KM 距離不會太遠，且因機動式干擾槍的功率皆不會太大。

以表 3 干擾槍的規格來計算 2.4G 為 58dB 630W 來計算大約 500 公尺為大多數的干擾槍 2.4G 遙控器干擾距離。

表 4、2.4G 發射功率與距離

發射頻段為 2.4G 計算出發射功率干擾無人機型式			
發射功率(dBm)	發射功率(W)	飽和距離	適用無人機型式
58.02 dBm	633 W	500 公尺	微型無人機
64.04 dBm	2.5 KW	1KM	微型無人機
70.02 dBm	10 KW	2KM	小型無人機
73.58 dBm	22 KW	3KM	中型無人機

(資料來源：本研究整理)

頻率為 5800MHz 因波長較短且干擾較多所以一樣功率傳輸距離更短，先以 0.1 公里(100 公尺)為計算範圍，則可計算出；

$$P_t = P_r - G_t - G_r + PL(32.44 - 20 + 75.26)$$

$$P_t = -30 - 3 - 3 + (87.7) = 51.7(\text{dBm}) = 147.9\text{W}(100 \text{ 公尺})。$$

$$\text{如果當距離為 } 200\text{m} \text{ 時，則 } P_t = 57.72(\text{dBm}) = 591.56\text{W}(200\text{m})。$$

$$\text{如果當距離為 } 300\text{m} \text{ 時，則 } P_t = 61.24(\text{dBm}) = 1.3\text{KW}(300\text{m})。$$

$$\text{如果當距離為 } 500\text{m} \text{ 時，則 } P_t = 65.68(\text{dBm}) = 3.70\text{KW}(500\text{m})。$$

因此以禁航區無人機的干擾槍要後要干擾 5.8G 圖資傳輸鏈路(傳輸距離短)，5.8G 並非遙控器的頻段而為圖資傳輸鏈路。

以表 3 干擾槍的規格來計算 5.8G 為 42dB 15.849W 來計算

$$P_t = P_r - G_t - G_r + PL(32.44 + 20\log D(\text{km}) + 75.26)$$

$$42 = -30 - 3 - 3 + (107.7 + 20\log D(\text{km}))$$

$$20\log D(\text{km}) = -29.7 \quad \log D(\text{km}) = -1.485 \quad D \text{ 計算出數值為 } 33 \text{ 公尺}$$

大約 33 公尺為此型干擾槍 5.8G 圖資傳輸干擾距離。

表 5、5.8G 發射功率與距離

發射頻段為 5.8G 計算出發射功率干擾無人機型式			
發射功率(dBm)	發射功率(W)	飽和距離	適用無人機型式
51.7 dBm	147.9 W	100 公尺	微型無人機
57.72 dBm	591.6 W	200 公尺	微型無人機
61.24 dBm	1.3 KW	300 公尺	小型無人機
65.68 dBm	3.7 KW	500 公尺	中型無人機

(資料來源：本研究整理)

4.2.2 反制無人飛行載具無線電阻斷策略(等效全向輻射功率)

在國家通訊傳播委員會電信技術中的低功率射頻器材技術規範 4.10.1.3 天線增益限制：操作於 2400 MHz~2483.5 MHz 頻段；進行固定點對點操作時，發射天線的方向性增益超過 6 dBi，每超過 3 dBi，最大傳導輸出功率限制值應降低 1 dB；一般商用無人飛行載具的 EIRP 規格均 $\leq 30\text{dBm}$ ，不會大於 32dBm。

$$EIRP = P_t + PL - Gr \quad (5)$$

將 4.2.1 相關 P_t (dBm) + PL (dB) 帶入上述公式則 EIRP 應為：

所以當 D 為 0.5Km，F 為 2400MHz，天線增益以 6 dBi 則

$$\bullet \quad EIRP(\text{dBm}) = P_t(\text{dBm}) + PL(\text{dB}) - Gr(\text{dBi})$$

$EIRP(\text{dBm}) = 58.02 + (-94.02) - 6 = -30$ ，所以是指如果以接收機去量發射機的 EIRP 則為 30 dBm。

所以當 D 為 1Km，F 為 2400MHz，天線增益以 6 dBi 則

$EIRP(\text{dBm}) = P_t(\text{dBm}) + PL(\text{dB}) - Gr(\text{dBi})$
 $EIRP(\text{dBm}) = 64.04 + (-100.04) - 6 = -30$ ，由上式得知所計算的 EIRP 均在符合規範 $\leq 30\text{dBm}$ 內。

4.2.3 反制無人飛行載具 GPS 導航失效策略

依上述的原理公式相關的功率及依照禁航區所律定的距離計算出，干擾控制訊號是指干擾無人飛行載具與操作者的遙控訊號。

干擾定位訊號是指干擾無人飛行載具的 GPS 定位導航訊號。因為 GPS 訊號對軌道衛星依賴性高，為了加強無人飛行載具對 GPS 訊號的接收強度，進而精準定位，一般無人飛行載具會設計定位天線主瓣在無人飛行載具上方，以利接收衛星訊號。使無人飛行載具對地面發射的干擾訊號有一定訊號接收不良情況，需要干擾時必須找到適合訊號點及相關位置。但現在也不是問題，因為不論商用無人飛行載具，還是軍用無人飛行載具，都會有特定作用，只需找出較通用頻段及發射功率，就能順利讓無人飛行載具失效或落地。

再把方程式(2)與方程式(3)整理 $P_t = P_r - G_t - G_r + PL$

先以 0.5 公里(500 公尺)為計算範圍，頻率為 1575MHz，則可計算出；

$$P_t = P_r - G_t - G_r + PL \quad (32.44 - 6.02 + 63.94)$$

$$P_t = -30 - 3 - 3 + (90.36) = 54.36(\text{dBm}) = 272.90\text{W}(500 \text{ 公尺})。$$

如果當距離為 1Km 時，則 $P_t = 60.38(\text{dBm}) = 1.09\text{KW}(1\text{Km})。$

如果當距離為 2Km 時，則 $P_t = 66.40(\text{dBm}) = 4.36\text{KW}(2\text{Km})。$

如果當距離為 3Km 時，則 $P_t = 69.92(\text{dBm}) = 9.81\text{KW}(3\text{Km})。$

表 6、GPS 1575M 發射功率與距離

發射頻段為 GPS 1575 MHz 計算出發射功率干擾無人機型式			
發射功率(dBm)	發射功率(W)	飽和距離	適用無人機型式
54.36 dBm	272.90 W	500 公尺	微型無人機
60.38 dBm	1.09 KW	1KM	微型無人機
66.40 dBm	4.36 KW	2KM	小型無人機
69.92 dBm	9.81 KW	3KM	中型無人機

(資料來源：本研究整理)

因此以禁航區的干擾槍干擾完遙控器，則干擾 GPS 訊號，但因為干擾槍的機動性要高無法太大功率且超過 3KM 已經很大了。

以表 3 干擾槍的規格來計算 1.575G 為 49.9dB 97W 來計算大約不到 300 公尺為干擾槍 1.5G GPS 干擾距離。

4.3 反制無人飛行載具直接摧毀策略

因商用型的無人機成本較低廉，如運用武力直接摧毀其實並不划算，而且有些無人機入侵禁航區可能不只一台，也常常有群體的無人機需結合多重反制手段，以下就介紹三種「硬殺方式」的優缺點。

一、反火箭、砲彈與迫擊砲系統：

(一) 優點：可保護基礎設施，可針對較大規模數量的無人機進行摧毀，用以作戰。

- (二) 缺點：會造成較大範圍及規模的破壞，且大概都是用於軍事用途，如圖 16，此系統使用火箭砲方式設置於船艦上，在海上可直接摧毀。



圖 16、船艦的反火箭系統圖示

(資料來源：文獻[28])

二、雷射及榴霰彈武器精準打擊無人機：

- (一) 優點：無論是雷射或榴霰彈還是軍事為主，能夠對於單一較大型的無人機進型摧毀，如圖 17，此系統使用雷射武器方式設置於船艦或是車載上，如在路上遇無人機實施偵查則使用雷射摧毀。
- (二) 缺點：此武器系統必須有相關雷達、紅外線、雷射槍等大功率的武力支撐。



圖 17、船艦的雷射武器系統圖示

(資料來源：文獻[29])

三、 捕捉槍網無人飛行載具：

- (一) 優點：對於小型的無人機可進行捕捉，適用於機場小範圍的反制無人機，成本較低；機動性高等，如圖 18，此系統使用網子方式直接用網子讓無人機落於槍網上。
- (二) 缺點：捕捉的距離較短(大約不會超過 50 公尺)、只能對單一無人機進行攻擊，此方法使用捕捉槍發射網子，將無人機直接網住摧毀無人機。



圖 18、捕捉型無人機

(資料來源：文獻[30])

第五章 結論與展望

5.1 結論

本文研究利用無線電的自由空間損耗及等效全向輻射功率計算出數據資料，依據數據資料計算干擾無人機時所需之功率與距離，並驗證目前在國外有使用的干擾槍為例，計算 2.4G、5.8G 及 GPS 的干擾距離大小及功率，但因 NCC【電波監理業務管理辦法】規定，如果未經合法申請頻段與功率則無法對其頻段進行干擾，【低功率射頻電機技術規範】規定如下【操作於 2400-2483.5 兆赫(MHz)，並至少使用 75 個跳頻頻道之跳頻系統及操作於 5725-5850 兆赫(MHz)之所有跳頻系統：1 瓦(W)(含)以下】，依本研究所計算出在機場內實施干擾時，干擾槍的數值均大於 1 瓦(W)，因此，如果有使用干擾槍研究的政府機關(構)、學校或法人及自然人，則必須先向 NCC 申請合法使用執照(無論無人機或是干擾槍)，方可合法使用。

5.2 展望

未來因應無人機相關威脅，我國應將無人機反制系統列為國家重要建設之一，並結合中科院相關技術，並加上民間力量與科技，並使機場的無人機防空系統能建置，以利互相支援。在國家發展無人機反制系統方面，同時結合多類型干擾或摧毀型的反制無人機系統，如反火箭、砲彈與迫擊砲系統，並多層部署，減少應付不對稱威脅成本，徹底消除無人機威脅，保護機場、重要關鍵基礎設施、重要軍政人員及政經中樞安全。

參考文獻

- [1]「反無人機技術創新 因應新興威脅」，《青年日報》，2021 年 3 月 10 日，檢自 <https://www.ydn.com.tw/news/newsInsidePage?chapterID=1341715&type=forum>
- [2]賴怡忠，「沙烏地油廠攻擊事件的戰略衝擊」，《芋傳媒》，2019 年 10 月 2 日，檢自 <https://taronews.tw/2019/10/02/476274/>。
- [3]交通部民用航空局，遙控無人機管理資訊系統，2021 年 7 月 13 日，檢自 <https://drone.caa.gov.tw/Default/DataList3>
- [4]國家通訊傳播委員會，電波監理業務管理辦法，2013 年 6 月 14 日，檢自 https://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=192&is_history=0&law_sn=2052&sn_f=2052
- [5]「2021 美國國防授權法案」，《Yahoo 論壇／邵宗海》，2020 年 12 月 30 日，檢自 <https://tw.news.yahoo.com/-yahoo%E8%AB%96%E5%A3%87%E9%82%B5%E5%AE%97%E6%B5%B7-2021-%E7%BE%8E%E5%9C%8B%E5%9C%8B%E9%98%B2%E6%8E%88%E6%AC%8A%E6%B3%95%E6%A1%88%E4%B8%AD%E6%B6%89%E5%8F%B0%E6%A2%9D%E6%AC%BE%E5%86%8D%E9%87%90%E6%B8%85-230037251.html>
- [6]D. Roy, Return of the Dragon Rising China and Regional Security, NewYork, PA Columbia University Press. 2013.
- [7]余雁翔，「遙控無人機危安防制」，《清流》，法務部，31 頁，2020 年 3 月。
- [8]M. Steven, "Armed Conflict In The 21st Century The Information Revolution and Post-Modern Warfare, PA Strategic Studies Institute, U.S. Army War College, 2000.
- [9]空軍航行管製手冊（第二版），國防部空軍司令部，中華民國，1-1-1-7 頁，2014 年 2 月。

- [10]航空通信助航設施技術規範，交通部民用航空局，180-188 頁，2012 年 3 月。
- [11]R. H. Scales, "Future Warfare.Carlisle, PA Strategic Studies Institute", *U.S. Army War College*, 1999.
- [12]舒孝煌，「國防情勢特輯 不對稱戰的演變與發展特輯 不對稱戰：反制無人載具的途徑」，財團法人國家安全研究院，2020 年 7 月。
- [13]S. J. Tangredi, *Anti-Access Warfare Countering A2/AD Strategies*.Annapolis, USA, 2013.
- [14]李騏嚴，通訊系統原理，全華科技圖書股份有限公司，台北，第 9.2-9.4 頁，1994 年。
- [15]林國榮，電磁干擾及控制，全華科技圖書股份有限公司，台北，第 2-5、10-14 頁，1998 年。
- [16]國家通訊傳播委員會，電信管理法，2019 年 6 月 26 日，檢自 <https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0060111>
- [17]粘添壽，電腦網路與連結技術，全華科技圖書股份有限公司，台北，2006 年。
- [18]「GPS 衛星大解密：從運作到使用」，《曾清涼》，2011 年 11 月 3 日，檢自 <https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=90b69989-4fd9-424b-946e-29fd6f610b31>
- [19]「反無人機技術及應用淺析」，《高端裝備產業中心》，2019 年 8 月 20 日，檢自 <https://kknews.cc/zh-tw/military/oe2223p.html>
- [20]「美國聯邦航空總署公布《無人機遠端識別最終規則》2021」，《資策會法律研究所》，2022 年 1 月 30 日，檢自 <https://stli.iii.org.tw/article-detail.aspx?no=55&tp=5&d=8605>
- [21]董光天，電磁干擾防制與量測，全華科技圖書股份有限公司，台北，2008 年。
- [22]S. R. Saunders, *Antennas and Propagation for Wireless Communication Systems*, USA: Wiley, 1999.
- [23]Draft revision of Recommendation ITU-R P.525-3 – Calculation of free space

attenuation, 2018, <https://www.itu.int/md/R15-SG03-C-0097>.

[24]陳俊仁。ISM 頻帶(2.412~2.483)系統電路實現，編著，2001 年 7 月。

[25]802.11-1999 - IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.2003,

<https://ieeexplore.ieee.org/document/1389197?tp=&isnumber=30234&arnumber=1389197&punumber=9543>

[26]陳威志，〈擴展障礙物環境下 MAV 偵察效能之無線通訊系統研發〉，碩士論文，國防大學理工學院電子工程研究所，第 25-32 頁，2013 年。

[27]「駿安科技」，檢自 <https://www.chinatimes.com/newspapers/20200525000467-260119?chdtv>

[28]「美艦首次以高能雷射擊落無人機反無人機技術及應用淺析」，《中時新聞網》，2020 年 5 月 25 日，檢自 <https://www.chinatimes.com/newspapers/20200525000467-260119?chdtv>

[29]「美首款雷射砲發射」，《ET today 新聞雲>軍武》，202 年 1 月 30 日，檢自 <https://www.ettoday.net/news/20170720/970118.htm>

[30]「東京警用無人機將以網具捕捉非法無人機」，《中時新聞網》，2015 年 12 月 30 日，檢自 <https://www.chinatimes.com/realtimenews/20151209004324-260408?chdtv>