

旅營指揮所無線廣域網路 應用與安全研析

作者／資訊作戰組教官 李武耀少校・國防部電展室資訊官 楊贊霖上尉

提要

一、全球互通微波存取是一種無線都會網路，由 WiMAX 聯盟所推動的無線寬頻協定，符合 IEEE 802.16 乙太網路介面標準。該科技提供高頻寬、長距離傳輸的無線寬頻技術，可改善傳統無線網路頻寬與距離的限制，並為缺乏網路基礎建設地區提供解決方案。

二、台澎金馬地形多變，城鎮建築增添通聯難度，多數地區無法單靠國軍現有通資裝備完成戰場兵科協同作戰需求，對長距離與高頻寬之裝備需求日增。

三、陸軍數位化旅主要的挑戰在於如何讓所有陸軍部隊能達成兵科協同作戰，使資傳持續保持通聯，其規格須滿足多用戶、多單位構聯，跨域通訊不中斷，寬頻視訊化與資傳安全化等條件，讓所有戰場物件皆能上國軍數位鏈路中，不管部隊是定點或是行動，命令下達即時接收。

四、鑑於指揮所因應平戰時諸般狀況，考量指揮所位置之隱匿性，且不受限於地形對通聯所形成之障礙，本研究採 WiMAX 通資平台結合保密器之研究作為參考。

前言

今年四月 21 日總統馬英九先生與 Intel 公司達成以 WiMAX 技術來建構 M 化台灣的政策宣示。隨後，在六月 2 日至 6 日台北世貿展中，關於 WiMAX 的產品展覽共計有全球六十家 WiMAX 業者聯合參展，展示最新的 802.16e 移動式 WiMAX 研發產品、測試方案與服務運用。

什麼是 WiMAX？對未來通資電產業有什麼重大的影響？用一個例子來說明其重要性。山上的原住民小學地處偏遠，網路基礎建設無法建構到該地區，然而，孩子需要教學資源與網路環境該怎麼辦？位於南投的暨南大學利用 WiMAX 微波技術將大學所擁有的網路資源連線到山上的小學，讓原住民孩子能享受與平地小學一樣的網路環境與資源，同時，促進國小的校務網路化。更多的企業廣泛地使用 WiMAX 充當中繼連線，解決缺乏通信基礎設施的環境問題，提供遠端建築物或特設的辦公據點連網，滿足不同據點即時通信，應用於緊急救援之臨時指揮所開設。

陸軍目前執行數位化旅的計劃，其主要的挑戰不在於讓一個單位全面數位

化，而是如何讓所有陸軍部隊能達成兵科協同作戰數位化、行動化，保持資傳通聯，小至單兵或武器載台，大至後勤補給，完全在數位鏈路中，不管是定點或是行動，隨時連網，命令下達沒有延遲，這是陸軍未來的目標。藉由 WiMAX 行動展示，配合國家政策推展，這是陸軍數位化的契機，將成為一具體可行的方案。

在中共對我情蒐日增，以及衛星偵照技術日新月異的情況下，指揮所面臨位置隱匿性與通聯性的取捨；隱匿性的需求是為防敵偵獲攻擊，通聯性的需求是為暢通指管鏈路，為避免指揮所牽就通信暢通，受限可用位置選項，本論文希提供一解決方案，運用 WiMAX 通信技術結合保密器達到兩項目標：一是強化指揮所通資能量與彈性，二是傳輸與保密安全，透過此安全模式運用之研究，提供本軍未來建軍通資技術參考。

本文

一、WiMAX 介紹

全球互通微波存取¹ (Worldwide Interoperability for Microwave Access, WiMAX)是無線都會網路(WMAN)，提供高頻寬、長距離傳輸的無線寬頻技術，可望改善傳統無線網路的限制，並為缺乏網路基礎建設地區提供解決方案。

WiMAX 符合 IEEE 802.16 乙太網路介面標準，最大傳輸距離為五十公里，頻寬為 20MHz，資料傳輸速率逼近 75Mbps。也就是說在區域作戰半徑五十公里內，區分近端通聯與遠端通聯；近端通聯約略為十二至十五公里，低頻寬區段，非視距傳輸 (Non Line-of-Sight ; LOS) 的傳輸品質足可支援作戰任務；遠端通聯約略為十五至五十公里範圍，惟有視距傳輸 (Light-of-Sight; LOS) 可支援作戰任務。WiMAX 提供偏遠單位長距離數據傳輸或區域範圍內的無線上網，為未來陸軍數位化的整合利器。

二、WiMAX 發展

美國電氣和電子工程師協會所 (IEEE) 設立 802.16 工作小組研發寬頻無線接入技術標準，802.16 系列標準發展藍圖，分為三個階段，第一階段是固定無線寬頻，以無線寬頻數據機為主要產品；第二階段是移動無線寬頻，以筆記型電腦內建無線上網模組為主要產品；第三階段是行動無線寬頻，以手機手持式產品為主要搭配。

¹ WiMAX 資訊網，[Http://wimax.tw/blogs/news/archive/2007/11/30/whats_WiMAX_technology.aspx](http://wimax.tw/blogs/news/archive/2007/11/30/whats_WiMAX_technology.aspx)。

目前推動 WiMAX 廠商品片組大廠計有：Intel、Redline 和 Wavesat。電信業者：北電（Nortel）、阿爾卡特（Alcatel）的行動網路建置。

802.16 系列相關標準比較如下表：

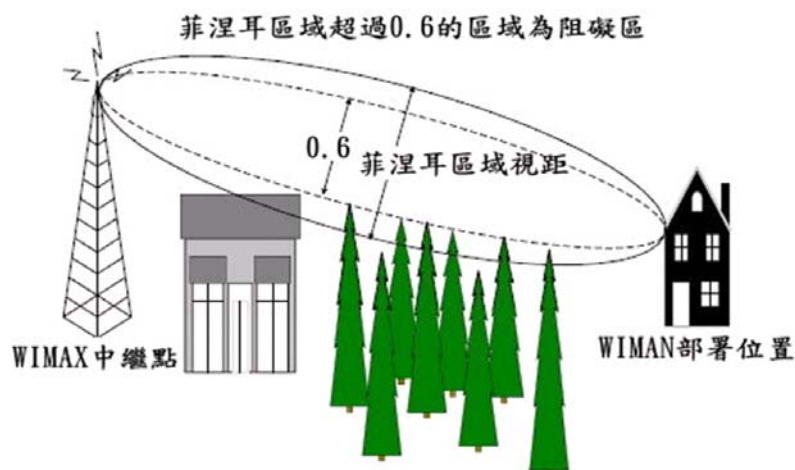
表一 802.16 系列相關標準比較表

標準	802.16	802.16a 802.16d (802.16-2004)	802.16e(802.16-2005)
底定時間	2001 年 11 月	2003 年 1 月/2004 年 6 月	2005 年 11 月
使用頻段	10-66GHz	<11GHz	<6GHz
頻段條件	視距傳輸	視距傳輸 非視距傳輸	非視距傳輸
傳輸速率	32-134 Mbps in 28MHz channel	75Mbps in 20MHz channel	Up to 15Mbps in 5MHz channel bandwidth
調變模式	QPSK, 16QAM, 64QAM	OFDM 256 ,OFDMA 16QAM,64QAM,QPSK,BPSK	同左
行動性	固定性	固定性和行動性	行動性
半徑	1~3 哩	3~5 哩,最大 30 哩	1~3 哩

(資料來源：The Standard of IEEE 802.16e,
<http://grouper.ieee.org/groups/802/16/published.html>)

三、WiMAX 技術

WiMAX 提供高速雙向網際網路連線，長程連線速度最快可達每秒 75 百萬位元 (Mb)。大部份的固定寬頻無線通信系統，均使用視距傳輸信號傳播，信號必需直接，不能受阻擋的傳送至接收端，信號傳送的淨空範圍需符合 0.6 倍的 1st Fresnel zone，Fresnel zone 因頻率與傳輸距離而定(圖一)。



圖一 菲涅耳區域視距傳輸示意圖

(資料來源：WiMAX Forum, <http://www.WiMAXforum.org/technology/downloads/WiMAXNLOSgeneral-versionaug04.pdf>)

菲涅耳區域²(Fresnel Zone)主要描述電磁波自發射端 (Transmitter, TX) 傳達至接收端 (Receiver, RX)，所發出電磁波能量應被限制於發射端天線的訊號角錐 (Signal Cone) 中，最短的路徑就是兩點之間的直線，當然電磁波也會向其他偏角處發射，如果這些偏角發射的電磁波沒有遇到任何阻礙，則它永遠也到達不了接收端，萬一遇到了障礙物，它就會反射回來，而再回到接收端，而當它到達接收端時，將會與循最短路徑到達的電磁波有不同的相位角，造成破壞性干擾，使得信號能量減弱。

WiMAX 802.16 信號傳送除支援視距傳輸之外，在 802.16a~802.16f 協定中均支援非視距傳輸，也就是說信號透過反射、散射與折射到達接收端，這樣的信號相對於直接波有不同的極性、延遲、衰落與穩定度等問題的探討，如何利用這些多路徑信號是能否達成服務的關鍵所在。

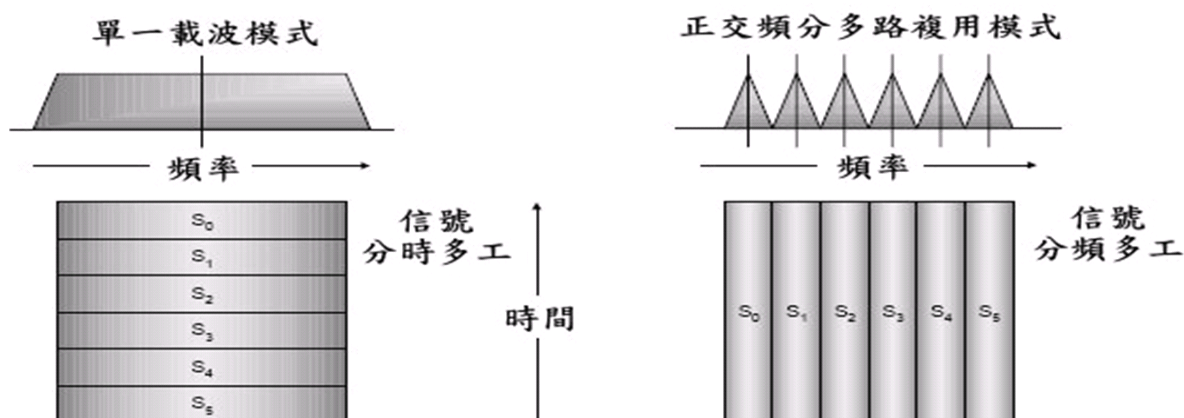
因此，WiMAX 克服多路徑衰落所造成信號不穩定的問題：

(一)正交分頻多工存取技術

正交分頻多工存取³ (Orthogonal Frequency Division Multiple Access, OFDMA)是多載波數位通訊調變技術，選擇正交載波作子載波(sub-carrier)，同時，利用多個子載波平行傳輸。如圖二左，單一載波模式依時間被順序送至接收方，使用單一載波調變至固定頻寬範圍內。

² WIKIPEDIA，[Http://en.wikipedia.org/wiki/Fresnel_zone](http://en.wikipedia.org/wiki/Fresnel_zone)。

³ WiMAX Forum, <http://www.WiMAXforum.org/technology/downloads/WiMAXNLOSgeneral-versionaug04.pdf>

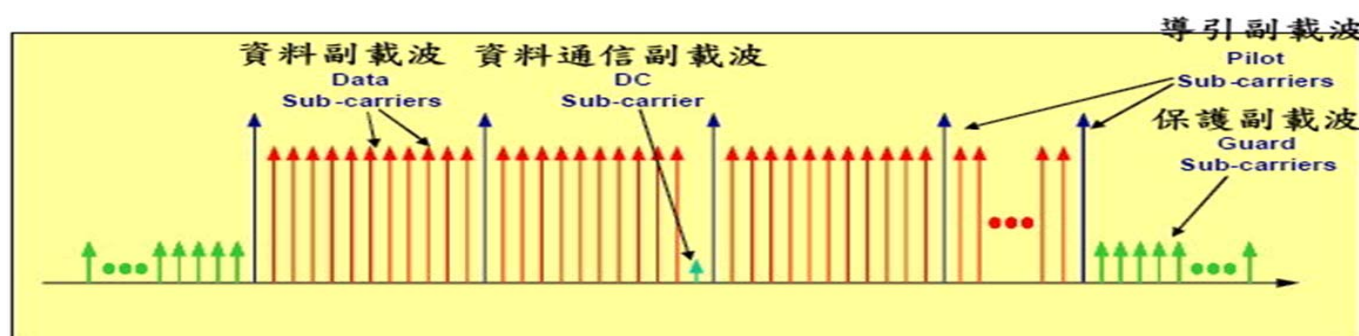


圖二 OFDM 單一載波模式、發送波形圖

(資料來源：WiMAX Forum, <http://www.WiMAXforum.org/news/downloads/WiMAXNLOSgeneral-versionaug04.pdf>)

圖二右為 OFDMA 的發送波形，在固定頻寬範圍內有許多的子載波，每一字符(symbol)被傳送的時間較長，對應使用頻寬較窄，因此能克服信號因傳送引起的延遲，一般常使用等化器來改善頻率選擇性衰退(frequency selective fading)所衍生接收信號品質不良的問題。

快速傅利葉轉換(FFT)讓正交分頻多工存取技術得以具體可行，使 WLAN、DVB、DAB、WiMAX 等規格接二連三地均選擇 OFDMA⁴為主要運用的技術，並訂定為下一代無線通訊系統的標準，實現即時資料傳送之目的。



圖三 OFDMA 子載波結構圖

(資料來源：WIKIPEDIA, http://en.wikipedia.org/wiki/orthogonal_frequency_division_multiple_access)

(二)適應性天線系統⁵ (Adaptive Antenna Systems, AAS)

WiMAX 使用多方向性天線能夠提供較高的增益，並可以接收多重路徑信號(Multi-path)，根據用戶訊號有不同的空間傳播方向，分別提供不同空間通道特

⁴ Mobile01, <http://www.mobile01.com/topicdetail.php?f=18&t=129716>

⁵ Conniq.com, <http://www.conniq.com/WiMAX/aas.htm>

性，並運用數位訊號處理和陣列天線觀念，適合複雜電磁環境的通聯要求，同時可以自動根據訊號方向性來調整權重，對準目標訊號並適應性地即時追蹤訊號，同時抑制(或消除)干擾訊號，以強化接收品質並增加容量、擴大涵蓋面和提高傳輸速率。

(三)適應性調變技術⁶ (Adaptive modulation)

WiMAX 的調變方式計有：BPSK、QPSK、16QAM、64QAM 等不同的調變方式，可以依據不同的使用需求，再運用不同的調變方式，以節省頻寬，或增加傳輸容量，運用適應性調變技術可使頻譜使用的效率較高。

(四)錯誤改正技術⁷ (Error correction techniques)

在數位通訊系統中常運用數位編碼技術以提高位元傳輸的正確率。WiMAX 使用誤碼校正技術(Strong Reed Solomon FEC)，迴旋編碼(convolution coding)，與插入演算法來校正誤碼，無法校正的誤碼則利用自動重發射要求 (ARQ)來改善誤碼率。

(五)功率控制⁸ (Power control)

WiMAX 基地台發射導引信號(Pilot)給用戶端，可以從用戶端接收導引信號的品質，得知其間通道衰落狀況，因而控制傳送適當之功率至每一用戶端，以降低用戶功率消耗與各用戶間不同訊號及基地台與用戶間之干擾。在視距傳輸環境中，發射功率與傳送距離成正比，在非視距傳輸環境中，發射功率則視路徑的阻擋情況而定。

(六)雙工⁹ (Duplexing)

為了提高傳輸容量，改善信號處理能力與系統相容性，WiMAX資料傳輸支援雙工技術，支援「同一頻帶雙工傳輸 (TDD)」及「相異對稱頻帶雙工方式 (FDD)」技術。

(七)靈活通道 (Flexible Channel sizes)

IEEE 802.16-2004 及 IEEE 802.16^e-2005 標準使用 3.5MHz、5MHz、10MHz 等頻寬，因此可整合至國軍頻譜管理作業規定內，在不同作戰環境，選用不同的通聯頻寬，例如：在城鎮作戰中，使用較高頻寬，提供較高傳輸速率；在山地特種作戰中，使用較低頻寬，提供較低傳輸速率，以符合作戰需求。對於作戰行動轉進過程中，也能在不同的系統中進行漫遊，具有自動調整頻寬的功能。

⁶ ZDNET, <http://whitepapers.zdnet.com/abstract.aspx?docid=108937>

⁷ 同註三。

⁸ 同註三。

⁹ 同註三。

目前寬頻連線以 T1、xDSL 或纜線數據機擔任主要網路選項，WiMAX 這項技術的出現提供更彈性的作戰運用，更節省建置時效。

WiMAX基地台以單點對多點的無線網路，初期的應用為連接戶外用戶設備；第二階段直接連接戶內用戶設備；最後的目標則是連接到可移動裝置如筆記型電腦、PDA與其他各式無線手持裝置，基地台再以點對點傳輸經由遠方中繼連上國軍骨幹網路。



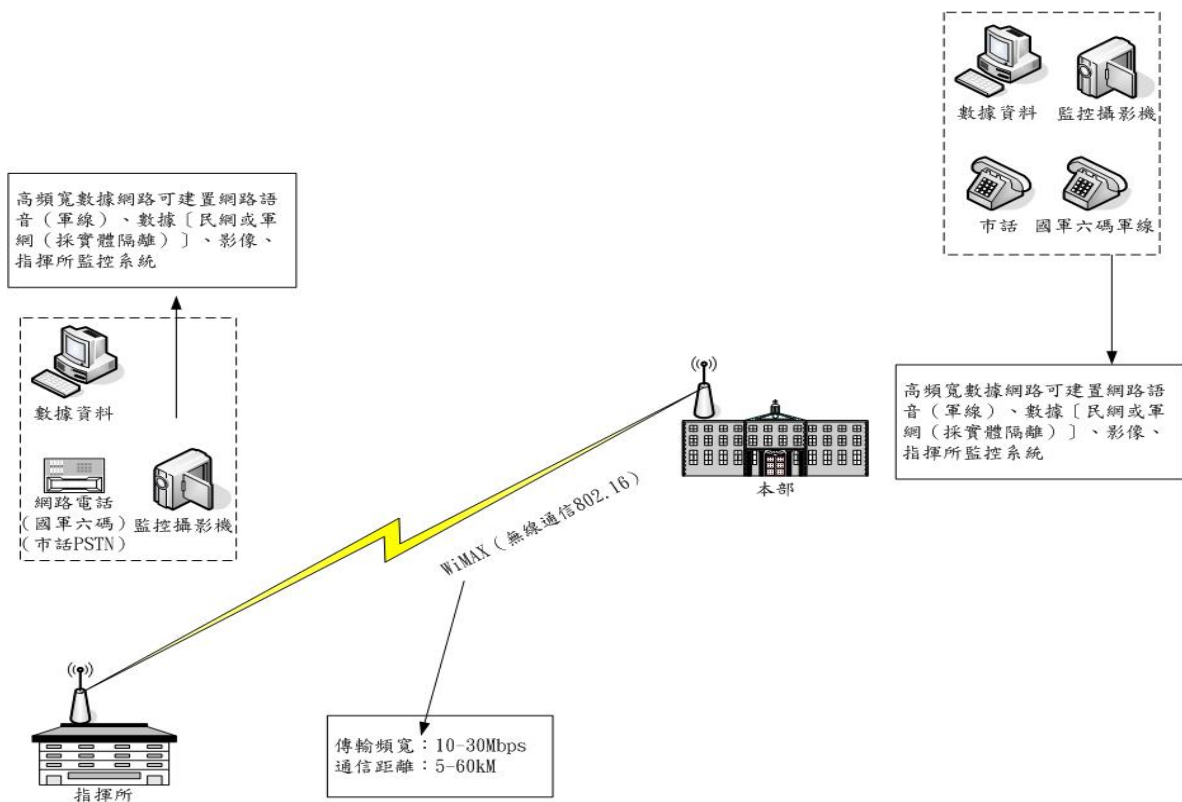
圖四 WiMAX 網路微波天線展示圖
(資料來源：WiMAX Forum, <http://www.WiMAXforum.org/product>)

四、通訊安全規劃

本文研究採WiMAX通信技術結合保密器應用於指揮所，因指揮所的開設位置與距離各種不同條件下，大致區分為兩種連線架構模式，分為無線-無線通信架構及無線-有線通信架構，分述如后：

(一)無線-無線通信架構¹⁰

在可達視距傳輸之範圍內，此架構適用於指揮所與附近營區直接作指管通聯，假若指揮所選定之地點與附近營區中間沒有任何障礙物，則利用WiMAX長距離通聯的本質，將資料直接以無線傳輸的方式傳送回營區內，結合營區現有的資源，進行語音、市話、傳真、軍網與其它通信手段之構連，規劃架構(圖五)。



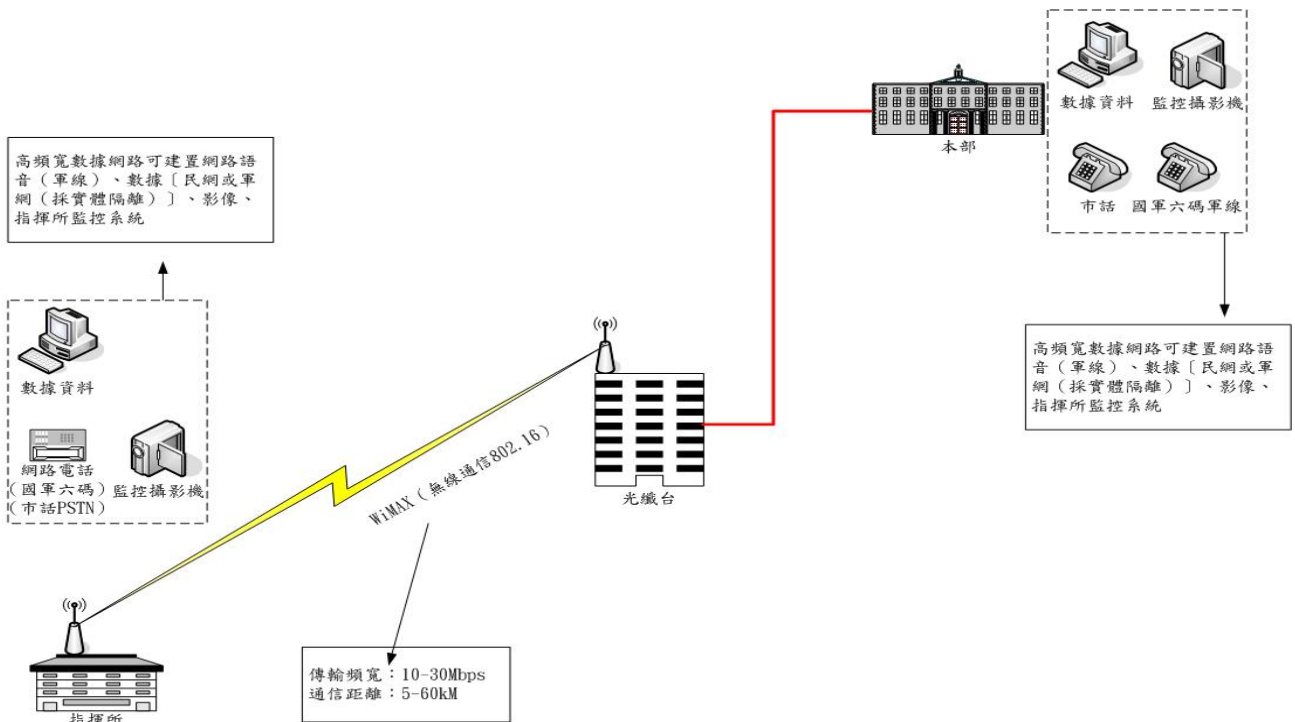
圖五 WiMAX 通信架構圖 (作者繪製)

(二)無線-有線通信架構

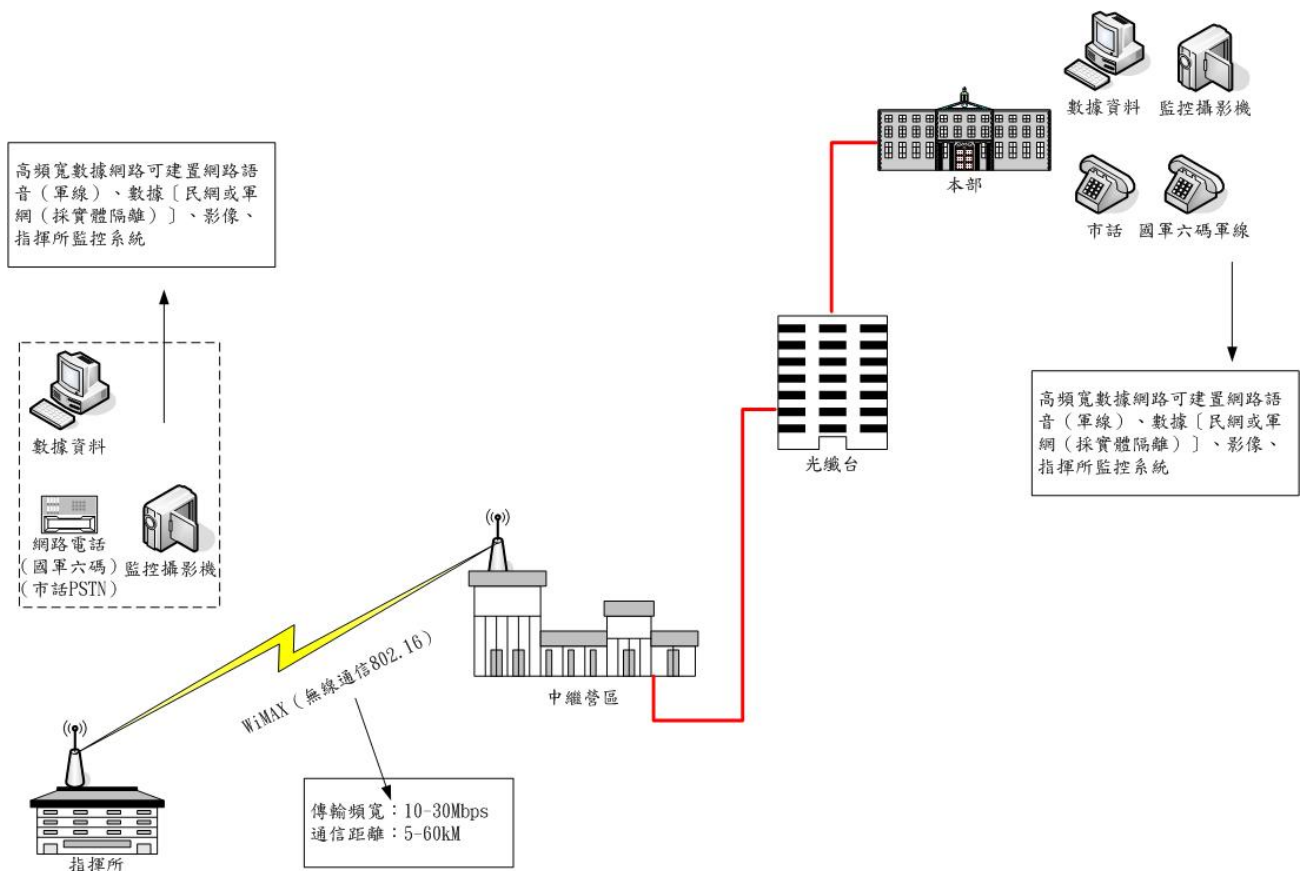
此架構適用於指揮所開設於較偏僻及隱密之位置，若指揮所附近存在光纖台(例如：員樹林的PCM A200 站台)可將指揮所以無線方式傳送至該台，再結合該台原有之有線模組將資料傳送回本部(圖六)；另開設之指揮所附近無存在之光纖台，可採由中繼營區將資料傳送至光纖台再結合該台之有線模組傳送回

¹⁰唐興家，「國軍資訊網路與戰術區域通信系統資訊網路整合路由設定之研究」，95年12月

本部(圖七)。



圖六 WiMAX 結合光纖台通信架構圖 (作者繪製)



圖七 WiMAX 結合中繼營區通信架構圖 (作者繪製)

(三)保密機制規劃架構

在傳統的觀念中，無線通訊頗受爭議性，許多洩違密事件的發生，皆認為與使用無線電波通訊不脫關係，雖然，無線通訊速度快，但訊號被截聽側錄與密碼破解的技術與日俱增，因此，在安全性上比實體線路差，本研究針對安全性問題規劃運用下列保密裝備規劃網路安全架構各式保密裝備如后：

1.WiMAX 無線模組¹¹：運用定向微波模組，且該設備應具鎖定 MAC 功能，以合法的 MAC 位址通過認證後才可連線，確保無線通訊安全。

2.使用制式保密器：採用中山科學研究院研製及國家安全局認可之制式保密器，本研究採用型號 EDU-05 VPN 保密器。

3.使用 UTM 防火牆¹²：該防火牆具虛擬私有網路(VPN)及入侵偵測系統(IDS)的功能，建立加密傳輸通道、監控與防護機制。

4.使用交換器(Layer 3)：於交換器上設定 ACL 存取權限控制，僅允許受信賴之網段存取內部網路資料。

5.使用認證伺服器¹³：認證伺服器(CA)是基於 PKI 體系的資訊安全系統，用以確認連線之電腦的身份程序，通過認證(即驗明正身)後，始得進入。

6.使用數位文件版權管理伺服器(DRM)¹⁴：所謂的 DRM(Digital Rights Management)乃是藉由電腦程式，限制數位內容使用方式的系統通稱；DRM 技術包括使用者認證、版權產生、驗證、移轉與權限管理等，使檔案傳輸獲得更佳的安全性。此加密機制在避免機密資訊遭竊取的主要防護技術，而加密是 DRM 軟體必備功能，其通常採客端(Client)與 DRM 伺服器軟體相互搭配，當文件加密時，終端程式就將文件金鑰與使用政策儲存在文件檔頭，併同使用者資訊與金鑰上傳伺服器，而另一使用者欲開啓該文件，須通過身分驗證後始能依使用政策閱讀。此外，大多數 DRM 軟體亦具備禁止列印的功能，並支援多種文書軟體格式，包括 Word、Excel、PDF、JPG 及動靜態網頁等，而更先進者尚可動態決定發行權限，並紀錄與稽核追蹤文件的存取、列印與閱讀時間等參數，管理者可巨細靡遺的檢視所有使用過程。

為提昇 WiMAX 通信技術之安全性需求，應妥善規劃保密裝備的架構。本研究之保密架構因選擇定向微波裝備且具鎖 MAC 功能，達到 WiMAX 基礎通訊安全，選用制式保密器更強化 WiMAX 通訊環境的安全性，運用具虛擬私有網路(VPN)及入侵偵測系統(IDS)功能的防火牆可有效阻擋由無線端進入的入侵，

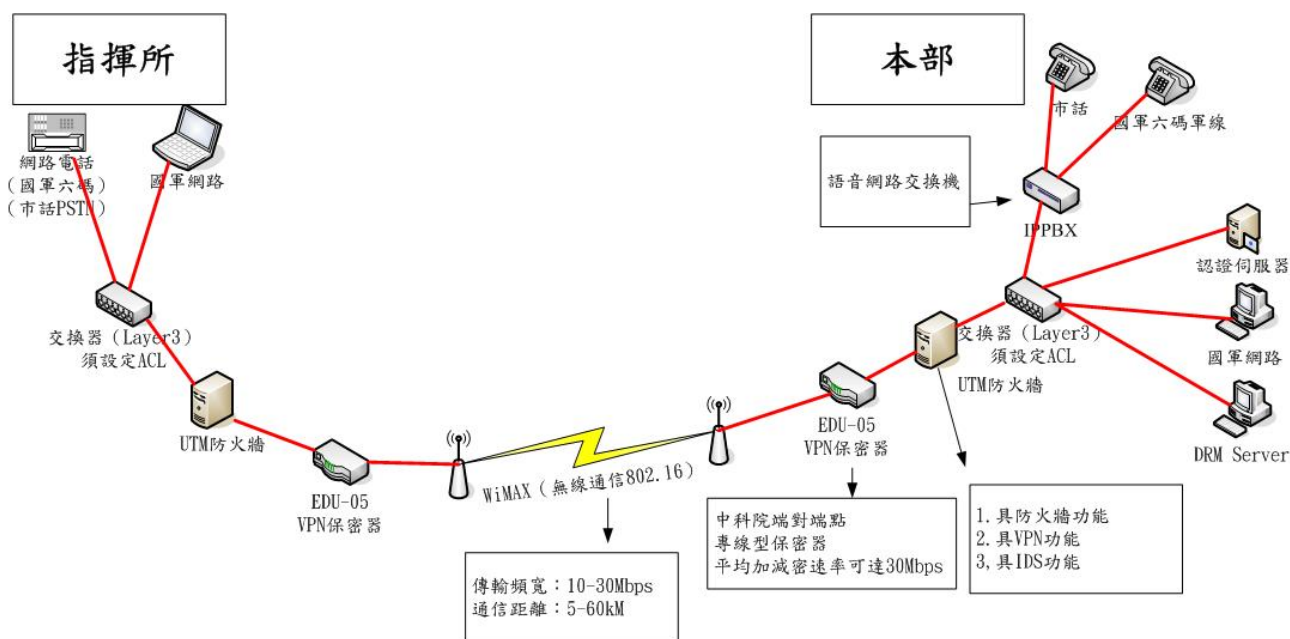
¹¹ Cyrus Peikari、Seth Fogie，「無線網路安全技術」，92 年 4 月

¹² 許建隆，「SSL 與 TLS 實務應用—架構全球網路的安全機制」，94 年 1 月

¹³ CA 認證系統應用，[Http://fourm.icst.org.tw](http://fourm.icst.org.tw)

¹⁴ DRM-機密數位文件版權管理標準介紹，[Http://www.ascc.sinica.edu.tw/94/2111/02.txt](http://www.ascc.sinica.edu.tw/94/2111/02.txt)

建立加密傳輸通道及時監控是否遭受入侵，並使用 Layer3 交換器可設定 ACL 存取權限控制，僅允許受信賴之網段存取內部網路資料，認證伺服器只允許經過認證之使用者登入軍網；數位文件版權管理伺服器（DRM）可有效達成使用者認證¹⁵、版權產生、驗證、移轉與權限管理等，使檔案傳輸獲得更佳的安全性，本研究之網路安全架構圖如下圖所示：



圖八 WiMAX 網路安全構想圖（軍民網實體區隔）（作者繪製）

五、未來安全防護

隨著通信技術的發展，先進的通信手段必須結合通資安全基礎建設，此為未來戰爭中攻守雙方必爭的目標，本研究之 WiMAX 通信技術結合保密器之創新架構，防護無線通信模式網路環境下可能之威脅，增加本軍未來於戰演訓時之通信能量，另急待努力與精進的方向。其具體作法如下所述：

（一）保密技術研發

國家安全局與中山科學研究院應致力研發無線通訊裝備保密器，提昇保密技術，加強國軍機動通訊能力；另運用無線通信技術時，使用保密器加強安全防護，並定期更換保密模組以確保通訊安全。

（二）管控部隊資安

強化部隊的通資安全設施與防護作為¹⁶，例如：更新伺服器硬體設施、安裝硬體防火牆實體隔離、安裝防毒軟體與弱點掃描系統、保持系統安裝最近的安

¹⁵ 葉世清，「機動戰術區域網路安全稽核模式之研究—以陸軍戰術區域通信系統為例」96年6月

¹⁶ Michael Palmer，「Guide to operating Systems Security」，96年6月

全更新、提防電子郵件的附件、安裝使用防火牆軟體、備份重要的檔案與資料夾、使用強健的密碼、提防下載的程式、安裝使用檔案加密程式並進行存取控制、使用 NAT IP 轉址功能、停用隱藏延伸檔名的功能等等。以確保平時及戰演訓時部隊的通資安全能量之建立，以達具體防護之效能，且盡可能部署專用伺服器、防火牆和路由器，若電腦和網路設備提供多樣化的功能，易遭受攻擊；故專用的伺服器和網路設備在管理上較簡單，且易於保護。

(三)加強資通能量

在技術方面應強化資訊管控人員熟悉各作業系統提供之安全性功能，如使用者帳號與密碼、群組安全性、權限、安全政策、帳號停用、安全協定、加密和認證；於心理層面應提昇幹部的通資安全意識。部隊的通資安全認知與防護是要靠平時單位內部全體人員一起去瞭解、遵守及維護，而非只靠資訊管控人員或系統維護人員獨自努力。如此，幹部經由通資安全教育獲得概念，方可提高部隊通資安全的防護，建立守法的觀念。

(四)策訂資安規範

訂定通資安全的規範是解決問題的根本之道，通資安全的規範與政策應是公開且經得起考驗。部隊有了通資安全的規範與遵循標準才能依法行政有所遵從。在平時或戰演訓時，才可循序漸進，按規範、按法令、按步驟、按要領(施行細則)，遂行部隊的通資安全相關規定。

結論

本研究於桃園機場實施無線廣域通聯測試，運用 WiMAX 通信技術結合保密器成功地驗證對指揮所指管通聯之可行性，同時，也讓人振奮地是今年所有的 WiMAX 廠商皆在推行動 WiMAX 通信，也就是車輛行駛中，指管通聯不中斷。換句話說，所有地面部隊在複雜電磁環境下進行兵種協同作戰時，凡在同一網路內的終端網路結點，不因作戰行動而中斷通聯，解決了陸軍數位化所遇到的許多瓶頸。當陸軍朝國家型計劃的方面來發展，基本上是配合國家政策的執行，除了植基技術於民間之外，更能發揮國家電子工業運用於國防的好處，不須依賴外國的軍售，更能長期發展國內國防工業。

未來最重要的成功要素是要有適當的無線網路頻譜管理與無線安全政策規劃，在適當的資安教育與教育推廣下，配合通資電整體規劃及科技發展趨勢，相信有一日台灣國防的通信能量能與世界強國並駕齊驅。