# 混亂編碼結合計數式一次密鑰技術運用在國軍無線網路環境整合之安全性研究

文／江宗慶 上尉・伍台國 所長・陳正鎔 助理教授


## 提要

超寬頻系統(Ultra-Wideband，UWB)是近年來非常受到注視的無線傳輸技術之一，該系統具有高傳輸速度、高容量、低功率消耗、低成本、低訊號攔截率等等之優點，可說是未來的明日之星，若能將之運用在國軍的資訊傳輸作業上，相信可對國軍各項任務的推行提供相當之幫助。本文將已可運用在UWB技術的PCTH機制為基礎，以結合混亂編碼及計數式一次密鑰技術的方法，將資料加密的方式融入PCTH機制中，讓該機制能具有資料安全的特性。此外本文也以海軍任務需求為背景，設計一可符合海軍作業的整合型網路環境架構，藉由此一架構，可擴展至全軍的無線網路環境整合設計上，希在未來國軍建置無線網路環境時可做為參考。

## 前言

隨著科技的日新月異，人類的生活也隨之變得愈來愈便利。近十年來，由於我們在通訊技術上的突破，讓原本須賴有線介質的傳輸環境，逐步變成不再受「線」所制的無線通訊環境，讓人可隨時隨地透過無線通訊網路，得到其所需要的各種資訊與技術。

然而，雖然無線通訊技術已爲我們帶來便捷的生活環境，但受限於無線傳輸所需使用的頻譜限制，在資料的傳輸速度及使用者的容量上，始終無法達到有線傳輸環境那樣的程度。此外，由於無線傳輸係依賴空氣做爲其資料傳送之介質，而生活中又隨時存在著各式各樣的電磁波，其所可能產生的干擾，也在在都是影響無線傳輸品質的要項。爲解決上述這些問題，就必須從無線傳輸技術的根本部分，也就是序列(Sequences)編碼方式來著手。

本研究之主要目的即是將用在無線傳輸編碼的混亂編碼技術(Chaotic Sequences)，結合使用一次密鑰技術運用在超寬頻脈衝無線電技術上，使其能在高速的傳輸中具有訊號難以被攔截及傳輸資料內容難以被破解之安全特性。相信以此技術可達到可靠性、安全性及資料的完整性，這尤其對我們國軍的任務需求最能發揮其功效。

有鑑於無線通訊需求的普及，不論是在資料傳輸速度或是使用者的容量上，均是無線通訊技術須突破的地方。近年來由於無線通訊需求的大幅成長，各項無線通訊技術不斷地被研究提出，以訊號涵蓋範圍來做區分的話，全球的無線通訊標準分類大致上可分爲：無線廣域網路(Wireless Wide Area Network,WWAN)、無線都會網路(Wireless Metropolitan Area Network, WMAN)、無線區域網路(Wireless Local Area Network, WLAN)及無線個人網路(Wireless Personal Area Network, WPAN)等。而本研究主要之目的，係將Chaotic Sequences的編碼技術，探討運用在最近剛提出來，適用在WLAN及WPAN的超寬頻無線電技術(Ultra-Wideband Radio Technology, UWB-RT)上。

UWB-RT是一種最近被提出來的無線通訊技術，它使用分享現存已知的頻寬，儘量降低訊號干擾現象，且具有訊號低衰減的特性，可達到降低裝置功率消耗及製作成本的效益。此外UWB-RT可在短距離的傳輸中達到100Mb/s以上的高資料傳輸率，也能選擇以降低傳輸率方式來增加連線的涵蓋範圍…等等，這些都是現有的WLAN或WPAN技術所欠缺的，而若要達到UWB-RT的效益，就必須從無線技術的根本編碼方式來做研究探討。Chaotic Sequences這種無線通訊編碼方式正是本研究的主要探討研究對象，藉由運用此種編碼方式，加強無線訊號的展頻(Spread-Spectrum)特性，以控制數位資訊的動態傳輸，讓UWB-RT達到低功率消耗、低干擾、削減多重路徑衰減、低攔截率及多使用者容量等之特性。

除此之外，爲增強傳送資訊的安全性，本論文也在資訊安全的部分同步做一研究。由於無線通訊所傳送之資訊極易被監聽及攔截，是以如何保護傳送資料的安全及完整性就變成了一項非常重要的工作。本論文將針對One-Time Password技術研究將其與混亂編碼技術中的Logistic Map結合，藉由One-Time Password的高安全性結合混亂編碼方法，令傳送的資訊更加難以被破解；此

外，本論文亦將就實務面部分，以海軍的無線作業環境需求，嘗試設計一個可適用於海軍的網路環境，希能達到國軍在無線通訊上對資訊安全之要求。

## 相關知識及背景

本論文所研究之對象，係運用在無線通訊系統裡的混亂編碼技術(Chaotic Sequences)，在混亂編碼技術中，本研究係以Bernoulli Shift Map與 Tent Map兩種編碼方式來產生傳送訊號所需之展頻碼；此外，在傳送資料部分，我們使用Logistic Map結合One-Time Password技術之方式將傳送資料加密，使該傳送資料具有難以被破解之特性；將此兩種技術運用到超寬頻無線電技術上，便可達到高速、安全、抗干擾及高容量的特性。以下即針對這幾個技術部分來做研究探討：

### 一、超寬頻無線電技術(Ultra-Wideband Radio Technology,UWB-RT)

近年來，我們在無線通訊技術的發展上有長足的進步，尤其是在無線廣域網路（包括GSM及3G等行動通訊系統）與無線區域網路部分，技術都已經相當成熟，然就無線通訊網路的整合而言，在短距範圍的個人網路部分(Personal Area Networks, PANs)迄今只有藍芽(Blue Tooth)技術的提出，但應用並不普及，原因正是其硬體元件成本過高，且傳輸速度受限(1Mb/s)，造成叫好不叫座的狀況，尤其是已進入3G時代，且正向4G時代邁進的現在，需要有更快、更好的無線通訊技術來滿足各項工作，而超寬頻無線電技術正是用來滿足短距離無線通訊需求（例如：室內網路、辦公室環境、大型的封閉式會場等等）的技術①。

UWB-RT係運用在短距離無線傳輸的技術，因UWB-RT乃是分享使用現有的頻寬，故其能整合現有的無線通訊系統，例如WWANs、 WLANs、 WPANs 及 WBANs (Wireless Body Area Networks)等，包括便攜式與固定式的無線通訊系統。目前在UWB的實體層設計上，主要就是要達到成本需求的降低及裝置功率消耗的減低，以達到經濟使用的效果，加上UWB在頻譜效率上的優勢，使得UWB可支援多媒體存取控制、允許在Multiple Hops間的Ad hoc通訊及可與有線的骨幹網路做無縫隙的連結存取，這對現在正快速發展的家庭網路及娛樂市場具有非常重大的影響。

由於UWB使用現有已知的頻寬，且可避免裝置間的訊號干擾（例如使用多重跳躍路由(Multihop Routing)，讓多個傳輸器可在所需地方同時運作），加上頻譜的再使用(Spectral Reuse)，使得每個使用區域的使用者容量增加，達到頻譜資源充分運用的效益②，且UWB可用在異質性網路的整合，讓固定式與便攜式的無線通訊網路得以整合。

UWB起初是運用在軍事的目的上，藉由其MIMO(Multiple Input Multiple Output)的特性，可提供系統的高可靠度與適應性。而隨著此一技術的商業化，UWB技術現在不僅可用在需高速率傳輸的無線個人區域網

① D. Porcino, and W. Hirt, " Ultra-Wideband Radio Technology: Potential and Challenges Ahead", IEEE Communications Magazine, (2003),pp.2-11.

② R. Popescu-Zeletin, Comp. Commun. Special Issue on Wireless World Research Forum, vol. 26, no. 1,(2003).

路，也能用在低速率但具有大量裝置的應用上，其目標就是著重在無縫隙共存的能力(Seamless Coexistence)、不同系統間的互相操作相容性(interoperability)及在不同無線通訊協定的整合(integration)，以達到異質性網路整合的目的。此外UWB也強調其操作介面對使用者而言是簡明易懂的，讓使用者能輕易的操作其相關裝置③。這對未來的通訊系統發展而言是非常重要的，尤其是系統的相容性與服務的並存性，須能保證在不同的裝置中也能維持應有之功能，而這部分就有賴在UWB設計時，建立PHY（Physical Layer-實體層）及MAC（Media Access Control,多媒體存取控制）標準的支援。

因具有以上的優勢，UWB-RT未來在短距離的無線通訊技術上，勢必有其發展的潛力，是我們可以好好深究探討的技術。

## 二、擬似混亂跳時編碼技術(Pseudo-Chaotic Time Hopping,PCTH)

Pseudo-chaotic是一種用來傳送數位資訊時，將該資訊編碼(coding)的方法，其原理是控制Chaotic Map的Symbolic Dynamics，得到想要的Symbolic Sequence（符號序列）④，以移除傳送訊號時可能產生週期的元件（即移除頻譜特性）方式⑤，來達到加強展頻特性的方法⑥。在此一狀況之下，傳送端本身與其他伺服器之間的干擾將可降低，例如與GPS(Global Positioning System)系統的干擾⑦，避免影響其他儀器之運作。

使用Pseudo-chaotic 來做傳送訊號的編碼可有效降低干擾的問題，但相對的在訊號接收端就必須要有能將其傳送訊號偵測出來，俾加以接收及解碼的功能，Viterbi Detector正是一種可以用來偵測Symbolic Dynamics編碼，並將之解碼還原的偵測器⑧。

由於Ultra-Wideband Impulse Radio(UWB-IR)超寬頻脈衝無線電系統係保障在短距離的無線通訊系統中，在設計低功率消耗(Low Power Consumption)、低攔截率(Low Probability of Intercept, LPI)、減低多重路徑衰減及增加使用者容量等功能時，降低其複雜度，而UWB-IR最新使用的編碼技術正是Pseudo Chaotic Time Hopping機制，以下就針對PCTH的特性及其編碼方式作一描述：

### ㈠PCTH之原理

#### 1. Shift Map及Bernoulli Shift

Shift Map是Chaotic System最簡單的範例，且擁有Chaotic Dynamic的所有特徵，其

③ T. G. Zimmerman, "Wireless Networked Digital Devices: A New Paradigm for Computing and Communication," IBM Sys. J. (Pervasive Comp.), vol. 38, no. 4, (1999), pp. 566-74.

④ B. Hao and W. Zheng, Applied Symbolic Dynamics and Chaos. Singapore: World Scientific,(1998).

⑤ N. F. Rulkov , and A. R. Volkovskii, "Threshold synchronization of chaotic relaxation oscillations," Phys. Lett. A, vol. 179, no. 4-5, (1993),pp.332-336.

⑥ G. M. Maggio, N. Rulkov, and L. Reggiani, "Pseudo-Chaotic Time Hopping For UWB Impulse Radio",IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS-I:FUNDAMENTAL THEORY AND APPLICATIONS,VOL. 48,NO.12,DECEMBER, (2001),pp.1424-1435.

⑦ R. G. Aiello, G. D. Rogerson, and P. Enge, "Preliminary assessment of interference between ultra-wideband transmitters and the global positioning system: A cooperative study," in Proc. National Technical Meeting of the Institute of Navigation,(2000).

⑧ G. D. Forney(1973), " The Viterbi algorithm," Proc. IEEE, vol. 61, pp. 268-273.

Symbol Space為：$\Sigma_2 = \{(s_0\ s_1\ s_2\ldots) \mid s_i=0 \text{ or } s_i=1\}$，其所對應之Shift Map為：

$\sigma : \Sigma_2 \rightarrow \Sigma_2$，$\sigma(s_0\ s_1\ s_2\ldots)=s_1\ s_2\ s_3$ .....(1)

其分散對應的狀態 $x$ 為：

$$x = 0.b_1b_2b_3\ldots \equiv \sum_{j=1}^{\infty} 2^{-j} b_j \quad \text{.....(2)}$$

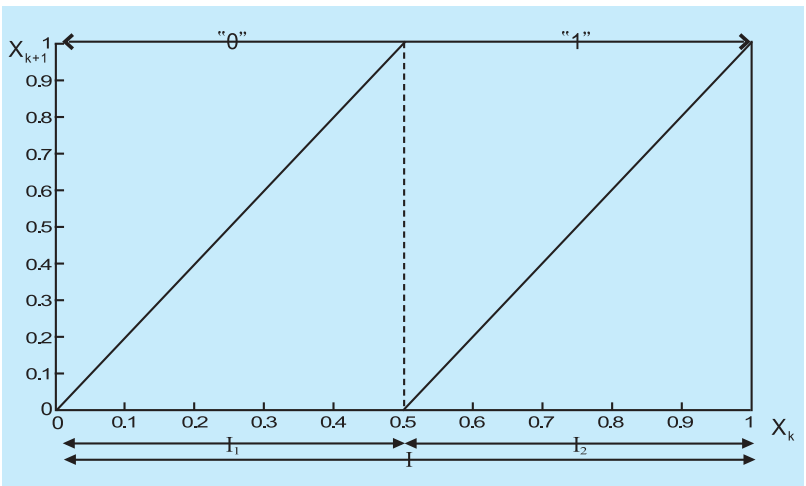
每個$b_j$位元為0或1，$x \in I = [0,1]$，此一Shift Map應用的二元序列 $\{b_j\}_{j=1}^{\infty}$ 由Bernoulli Shift Map做分散：

($x_{k+1}=2x_k$ modl 在 $x_k = 0$ 或 0.5 時，$x_{k+1} = 0$)...(3)

該Bernoulli Shift map 圖示如圖一，其中區間$I_1$及$I_2$均從0開始，以2的斜率增加。

2. Symbolic Dynamics

Symbolic Dynamics的觀念係將空間分割並將符號結合到分割的部分，故Dynamical System的軌道便可如同Symbolic Sequence般被分析，由此觀點，Chaotic System就可被看成自然資訊的來源。例如在圖一中，我們選擇I區間[0,1]為Markov Partition，其臨界點c=0.5，為了描述符號的Chaotic Map的動態，我們將二元符號0,1結合到子區間$I_1$及$I_2$中，故此Bernoulli Map的Symbolic Sequences即可描述為：S = {010010...}




圖一　Bernoulli Shift map

3. Pseudo-chaotic Encoder

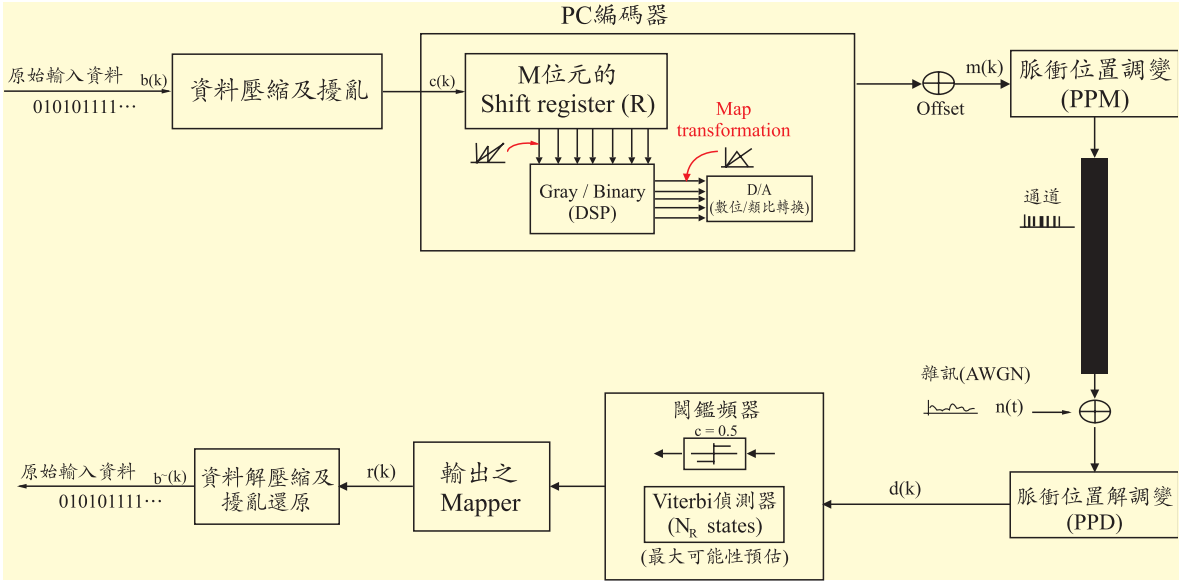
在此部分，Bernoulli Shift的程序是由有限長度轉換暫存器R (Finite-length Shift Register)來模擬，如圖二，R被c(k)提供二元資訊準備傳送，圖三說明使用最小有效位元(LSB)取代MSB（最大有效位元）的位置，我們假設二元串流c(k)提供給轉換暫存器R屬於i.i.d.之序列(Independent and Identically Distributed)，此法可由在R之前插入一資料壓縮及資料擾亂（雜亂）區塊來達到目的（圖二）。

由於R的長度有限，Bernoulli Shift的Dynamic只能近似，故一個M-bits的轉換暫存器一般表示為：

$$x = 0.b_1b_2b_3\ldots b_M \equiv \sum_{j=1}^{\infty} 2^{-j} b_j \quad \text{.....(4)}$$

$b_1$為MSB，$b_M$為LSB，此M-bit的量化誤差為：$\varepsilon(M) < 2^{-M} \Rightarrow M \rightarrow \infty\ \varepsilon(M) \rightarrow 0$

因Pseudo Chaotic的編碼能根據狀態定義方程式(4)來預控Bernoulli Shift方程式的Symbolic Dynamics，故Bernoulli Shift的Symbolic Dynamics是由在轉換暫存器R中的MSB的連續值所決定，意即在分隔點c右邊的第一個位元決定$I_1$或$I_2$中的反覆落點，而其他的位元則決定$I_j$的相關位置，但是在step k的MSB值會與在step (k-M)的LSB同時發生，依次地，LSB會包含c(k)的資訊位元，故PC 編碼即可依此性質來做預測。因此，若能適當應用此靈敏性來初始化Chaotic System的條件，就能控制它的Symbolic




圖二　PCTH機制的區塊流程圖

Dynamics，得到想要的Symbolic Sequences，而編碼方式產生之訊號可使用Viterbi 偵測器(VD)來執行ML解碼（當AWGN雜訊被加入時），以恢復已被編碼的訊號。

一般來說，Shift Register執行Bernoulli Shift Map是依照數位訊號處理(DSP)單位而做，以產生更複雜的Chaotic Map，這用在頻譜的shaping 及加強ML的偵測方面非常有用，因此我們使用Map的轉換公式：

$$X_{k+1} = 1 - 2|X_k - 0.5| \quad \text{.....(5)}$$

將Bernoulli Shift Map轉換成Tent Map，這麼做是爲了讓系統存在雜訊而使得map中的符號不連續的狀況下，讓系統具有更大的強健度。

㈡PCTH訊號(PCTH Signal)

在PCTH機制中，DSP（數位訊號處理）單位的輸出轉成類比的訊號(使用D/A轉換器，見圖三)，使用固定的補償(Offset)加到這個類比的訊號以形成調變訊號m(t)，俾使用到PPM（脈衝位置調變器）中。

㈢PCTH解碼器(PCTH Decoder)

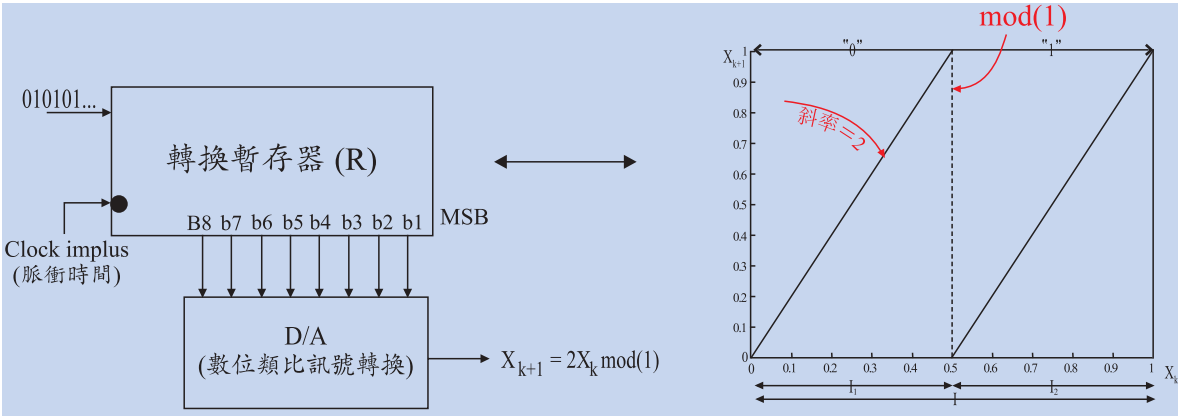
PCTH訊號是不使用載波(carrier-less)的訊號，因此在接收端沒有需要建立參考訊號來解碼資訊的必要，因此我們只能假設符號同步化是能被建立的。

1. 脈衝位置解調變(Pulse-Position Emodulation, PPD)

在圖三中，接收端包含一個PPD的步驟，意即在一個理想的接收端，脈衝訊號的理想偵測是由脈衝關聯器來比對脈衝波形的方法來達到目的。此一脈衝器（或是比對一致的濾波器）可在時間框架中偵測到每個傳送脈衝位置的存在，故可提供在接收訊號及$2^M$個每個可能的傳送訊號間之距離的測量。

2. 閾鑑頻器(Threshold Discriminator)

在最簡單的case中，二元資訊c(k)可在使用PPD輸出後的閾鑑頻器中被檢索，但當脈衝值與chaotic反覆值一致地接近Tent Map的分割點c(=0.5)時，可能會產生關鍵的錯誤元件，爲了降低此一錯誤元件產生的機率，在Chaotic Map的分割點c的周圍建立一個雜訊 "gap" （可使用線性編碼來避免連續




圖三　使用M-bits的轉換暫存器部署的Bernoulli shift map

的0串列出現）。此一限制通常是由run-length的限制，並由RLL(0,k)來表示（k指的是允許最大連續0值的數目）。

3. ML 偵測(ML Detection)

一般來說，對一個傳輸系統而言，最佳的接收器是依編碼及預測訊號的交織相稱而構成。對每個符號週期，偵測器應能判斷（估計）接收訊號及預測訊號之間的關聯，並根據編碼限制選擇具有最大相關的序列。最爲人所知的ML偵測器可應用Viterbi演算法來達到此一目的。也就是說Viterbi演算法允許接收到錯誤訊號的一部分的回復，意即可藉由偵測器本身來重現傳送訊息，以提供狀態的預估訊列。

總括來說，PCTH機制是利用Chaotic Map的Symbolic Dynamics來做數位資訊的編碼及將多層級PPM來調變到其通道上。而pseudo-chaotic調變則具有產生類雜訊頻譜的優點，這是一個可具有LPI及可降低與其他使用者之間干擾的需求特性。此機制是採使用標準Viterbi演算法的ML偵測的應用，與慣例使用的迴旋編碼比照起來，這個PCTH偵測器具有更高的性能擴充性，且在接收器的設計上可增加相當的彈性，未來若能將PCTH的應用延伸到實際的多使用者環境中，定可提供更具效能的UWB系統。

## 三、計數式一次密鑰技術

一次密鑰技術，顧名思義即是每次均使用不同的「認證資料」登入系統，以避免遭受非法使用者的僞冒攻擊。本文所要討論的是有別於一般僅具有Server對使用者身份單向認證功能⑨⑩的「計數式一次密鑰」技術，本文係以葉慈章等人所提出的可防止重送(Replay Attack)及阻斷服務攻擊(Denial of Service Attack)，並具有對Server及User雙方做雙重身份認證的一次密鑰認證技術(Yeh-Shen-Hwang's Scheme)爲基礎⑪，並針對TSUJI 及Akihiro SHIMIZU 所提出可以僞

⑨ 江宗慶，伍台國與陳正鎔，「改良式One-Time Password認證OSPA協定技術運用在海軍艦艇物料籌補申請作業之安全性研究」，第十二屆國防管理學術暨實務研討會，（台北：國防大學國管理學院主辦，2004）。

⑩ T. Tsuji , and A. Shimizu, "An impersonation attack on one-time password authentication protocol OSPA", IEICE Trans. Commun, Vol. E86-B, No.7 , (2003),pp.2182-2185.

⑪ T.-C. Yeh , H.-Y. Shen , and J.-J. hwang, "A secure one-time password authentication scheme using smart cards" , IEICE Trans. Commun. , vol.E85-B , no.11 , (2002),pp.2515-2518.

冒及竊取認證資料方式攻擊該One-time Password的方法⑫，重新設計一個能防止攻擊者利用攔截到的登入驗證資料，僞冒登入系統的「改良之計數式一次密鑰技術」⑬⑭。

計數方式的一次密鑰技術，最原始的是以Lamport password authentication method⑮⑯爲基礎而提出來的S/Key one-time password authentication system⑰，但因S/Key scheme極易遭到攻擊，是以葉慈章等人在2002年時提出另一以S/Key技術爲基礎而做出改良的Yeh-Shen-Hwang's scheme。但因該法遭到TSUJI及Akihiro SHIMIZU所破解，因此我們重新設計一新的計數式一次密鑰技術，其敘述如後：

㈠計數式一次密鑰技術所用符號及其定義

1. K：使用者的密碼。

2. H：單向(one-way)的雜湊函數。

3. N：使用者與系統註冊時，系統允許使用者最大可登入次數。

4. t：使用者登入系統的次數。

5. SEED：使用者向系統註冊時，由系統與使用者相互協定的密鑰。

6. D：系統隨機產生的亂數。

7. ⊕：XOR 運算符號。

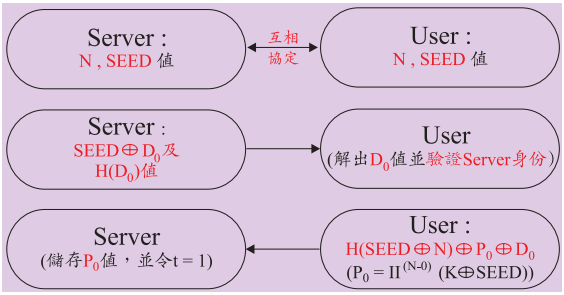
8. $P_t$：表示將K⊕SEED 之值做N-t次的雜湊，即$H^{N-t}(K⊕SEED)$，例如$H^3(K⊕SEED)$就是表示H(H(H(K⊕SEED)))。

㈡計數式一次密鑰技術的註冊階段(如圖四)

1. 伺服器將與User協定的密鑰 SEED 值及登入最大使用數N值傳送給使用者。

2. 伺服器再將 SEED⊕$D_0$，及H($D_0$)值傳送給使用者。

3. 使用者藉由SEED⊕$D_0$⊕ SEED = $D_0$算出$D_0$值，並將$D_0$值做hash，比對是否等於Server送過來的H($D_0$)，若相等則驗證Server身份爲合法，此時User將H(SEED⊕N)⊕$P_0$⊕$D_0$值($P_0 = H^{(N-0)}(K⊕SEED)$) 算出後回傳給伺服器，伺服器則藉由H(SEED⊕N)⊕$P_0$⊕$D_0$⊕H(SEED⊕N)⊕$D_0$ = $P_0$算出$P_0$值，並令t = 1，並將該二值儲存以做爲下一次使用




圖四　計數式一次密鑰技術的註冊階段流程圖

⑫ T. Tsuji , and A. Shimizu, "Cryptanalysis on one-time password authentication schemes using counter value" , IEICE Trans. Commun, Vol. E87-B, No.6 , (2004),pp.1756-1759.

⑬ 江宗慶，伍台國與陳正鎔，「改良之計數式一次密鑰技術運用在電子商務交易安全之研究」，第一屆創新與管理學術研討會，（台北：實踐大學主辦，2004）。

⑭ 江宗慶，伍台國與陳正鎔，「計數式一次密鑰技術結合改良式SET協定運用在網路信用卡交易安全之研究」，2005電子商務與數位生活研討會，（台北：實踐大學與台北大學合辦，2005）。

⑮ N. Haller, "The S/Key(TM) one-time password system" ,Proc. Internet Society Symposium on Network and Distributed System Security , (1994),pp.151-158.

⑯ L. Lamport, "Password authentication with insecure communication" , Commun. ACM , Vol.24 , No.11 ,(1981), pp.770-772.

⑰ T. Kamioka , and A. Shimizu, "The examination of the security of SAS one-time password authentication", IEICE Technical Report OFS,48,(2001).

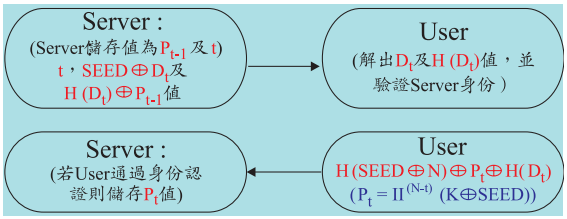
者欲登入系統時的身份認證資料。

㈢計數式一次密鑰技術登入階段(如圖五)

假設使用者爲第t次登入系統，此時Server儲存之值爲：$P_{t-1}$及t。

1. 伺服器(Server)將 t ， $SEED \oplus D_t$ 及 $H(D_t) \oplus P_{t-1}$ 值傳送給User。

2. User收到該值後，利用$SEED \oplus D_t \oplus SEED = D_t$及$H(D_t) \oplus P_{t-1} \oplus P_{t-1} = H(D_t)$算出$D_t$及$H(D_t)$，並將$D_t$做hash以比對是否等於$H(D_t)$，若是則驗證Server的身份，此時User即計算認證資料$H(SEED \oplus N) \oplus P_t \oplus H(D_t)$，並將該值傳送至Server辦理身份認證($P_t = H^{(N-t)}(K \oplus SEED)$)。



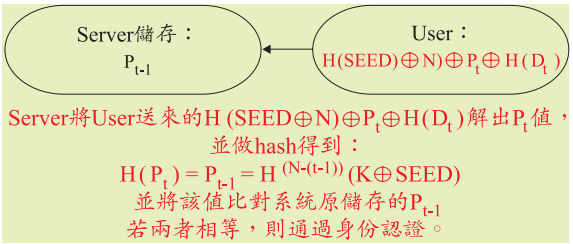

圖五　改良之計數式一次密鑰技術的登入階段流程圖

㈣計數式一次密鑰技術的驗證階段（如圖六）

伺服器接到使用者的$H(SEED \oplus N) \oplus P_t \oplus H(D_t)$值即利用$H(SEED \oplus N) \oplus P_t \oplus H(D_t) \oplus H(SEED \oplus N) \oplus H(D_t) = P_t$ 解出$P_t$，並將該值做hash以比對原先儲存的$P_{t-1}$，若$H(P_t) = P_{t-1} = H^{(N-(t-1))}(K \oplus SEED)$，則驗證User身份爲合法，允許User登入系統。此時Server將儲存的身份認證值改成$P_t$，下次登入的次數則爲t+1。

## 四混亂加密技術(Chaotic Encryption)

混亂編碼除了用在通訊上的訊號傳送




圖六　改良之計數式一次密鑰技術的驗證階段流程圖

外，因其混亂之特性，故亦可做爲加密技術之用⑱⑲，本文將提出一個以Logistic Map方式來對資料做加密的方法。

㈠Logistic Map是使用在Chaotic Systems 中的其中一種方法，其公式爲：

$X_{n+1} = r \cdot X_n(1 - X_n)$ ， $X_n \in [0,1]$ ，且$0 \leqq r \leqq 4$，在本文裡我們將r值指定爲4（因可產生在[0,1]之間的亂數），在資料的加密部分我們將使用兩個初始值來對資料加密並將加密後的資料順序打亂，如此不但能使資料本身具有加密效果，因其順序也被打亂，除非可正確將原始順序排列出來，否則即使知道如何解密也無法將資料還原回原來的型態（若資料有m個位元，則該資料的排列方式就有m!個可能）。

㈡首先我們要先指定兩個初始值INI1及INI2 ， 該二個初始值的選取範圍爲[0,1]，（由於Logistic Map的特性是只要初始值有一些些的差異，其所產生的序列就會有很大的不同，因此可用來加密的對象就可以說是趨近於無限）。我們令INI1爲$p_0$，INI2爲$q_0$，並將該$p_0$及$q_0$帶入Logistic Map公式中產生所需之序列$p_1,p_2,p_3...$及$q_1,q_2,q_3...$。

㈢接下來我們以式⑸產生對資料加密之序列：

⑱ M. S. Baptista, Physics Letters A 240(1998),pp.50-54.

⑲ A. Palacios , and H. Juarez, "Cryptography with cycling chaos" , Physics Letters A 303,(2002), pp.345-351.

$y_i = \text{int}(p_i * 255.0 + 0.5) \forall i = 1(1)n$ .....(5)

此處$p_i$*255+0.5是因爲要將加密值轉換成8位元，若要變成16位元則變成$p_i$*($2^{16}$-1)+0.5以此類推以產生所需的位元加密值。

㈣再接下來我們將要加密的資訊轉換成ASCII碼，並令其爲$c_1,c_2,c_3...c_n$(n爲資料個數)，並以式(6)將該值加密。

$m_i = c_i \oplus y_i \forall i = 1(1)n$ ..... (6)

㈤完成資料的加密後，我們要做的就是把此一加密後的資料順序打亂，故我們以第二個初始序列$q_1,q_2,q_3...$，利用式(7)產生新的序列順序。

$z_i = \text{int}(q_i * N + 0.5) \forall i = 1(1)n$ .....(7)

此處N = n。

㈥依照$z_i$產生之值重新由小取到大做排列，並將其對應到$m_i$，便可打亂加密後之資料序列，例如若$z_1$=2,$z_2$=3,$z_3$=1，則由小排到大的順序是$z_3,z_1,z_2$，對應到$m_i$則爲$m_3,m_1,m_2$，故新的序列即爲$m_3,m_1,m_2$，此一新的順序我們以$e_i$來表示，意即$m_3=e_1,m_1=e_2,m_2=e_3$。

㈦若要將資料還原，第一步驟就是先將$e_i$還原爲$m_i$，也就是從$z_i$的排序來做還原，例如$z_1$的排序爲2，故$m_1$就是$e_2$；$z_2$的排序爲3，故$m_2$就是$e_3$；$z_3$的排序爲1，故$m_3$就是$e_1$。

㈧在把加密後的資料序列還原後，接下來要做的就是將資料解密，我們令原始資料爲$d_i$，其解密還原公式爲：

$d_i = m_i \oplus y_i \forall i = 1(1)n$ .....(8)

㈨利用式(8)便可將資料還原爲原始狀態，再經過ASCII碼的對照便可解讀出原始資料的內容。

㈩範例

在此我們以假設要傳送navy這四個字母爲例，我們取INI1 = 0.28，INI2 = 0.82 做爲初始值，並令r = 4：

1. 由INI1 = $p_0$，並以 $X_{n+1} = r \cdot X_n(1 - X_n)$ 算出$p_1,p_2,p_3,p_4$分別爲：0.8064，0.6245，0.9380，0.1464。

2. 以式(5)算出$y_1,y_2,y_3,y_4$，其值分別爲：206，159，239，37。

3. 取ndmc的ASCII碼，其值分別爲：n=110=$c_1$，a=97=$c_2$，v=118=$c_3$，y=121=$c_4$

4. 以式(6)算出$m_1,m_2,m_3,m_4$，其值分別爲：160，219，153，92。

5. 由INI2 = $q_0$，亦以 $X_{n+1} = r \cdot X_n(1 - X_n)$ 算出$q_1,q_2,q_3,q_4$分別爲：0.5904，0.9673，0.1265，0.4420。

6. 以式(7)算出$z_1,z_2,z_3,z_4$，其值分別爲：3,4,1,2。

7. 將$z_1,z_2,z_3,z_4$，之值由小排到大，其順序爲$z_3,z_4,z_1,z_2$，與之對應到$m_1,m_2,m_3,m_4$，取得$m_3,m_4,m_1,m_2$，並令其爲$e_1,e_2,e_3,e_4$（意即$e_1=m_3,e_2=m_4,e_3=m_1,e_4=m_2$），此即爲以Chaotic Encryption加密後的傳送資料。

8. 若要將資料還原，首先我們根據$m_3,m_4,m_1,m_2$之順序將$e_1,e_2,e_3,e_4$取爲$e_3,e_4,e_1,e_2$，此一順序即爲$m_1,m_2,m_3,m_4$。

9. 要將$m_1,m_2,m_3,m_4$。還原爲$c_1,c_2,c_3,c_4$，只需以式(8)去做計算，即可得回原本的ASCII傳送數值，藉由對照方式即可將原本傳送的ndmc字母還原回來。

## 結合混亂編碼與計數式一次密鑰技術運用在超寬頻系統之模型

在前一章節所提到的PCTH方法，需要在轉換暫存器R之前提供一個符合M位元的傳送資料，因此我們設計以一次密鑰技術結合混亂加密的方式，將欲傳送之資料藉由此

一方式轉換成符合M位元的二元資訊碼，再藉由PCTH的傳送機制傳遞資料，以下爲其技術模型：一次密鑰技術結合混亂加密法。

一、藉由前章節的改良式OSPA協定技術由傳送（使用者端）及接收（伺服器端）雙方藉由安全通道完成註冊。

二、傳送資料之前，傳送端與接收端之間先藉由彼此連線的建立（使用一次密鑰的身份認證方式）確認彼此身份。

三、運用前章節之式(2)、(3)、(4)、(5)，並將式(4) $z_i = \mathrm{int}\left(q_i * N + 0.5\right) \forall i = 1(1)n$ 改變成下式：

$$z_i = \mathrm{int}\left(q_i * (N + (a_{n-1} * a_n)) + 0.5\right) \forall i = 1(1)n \quad (6)$$

此處的$a_{n-1}$及$a_n$即爲OSPA協定使用的身份認證資料。

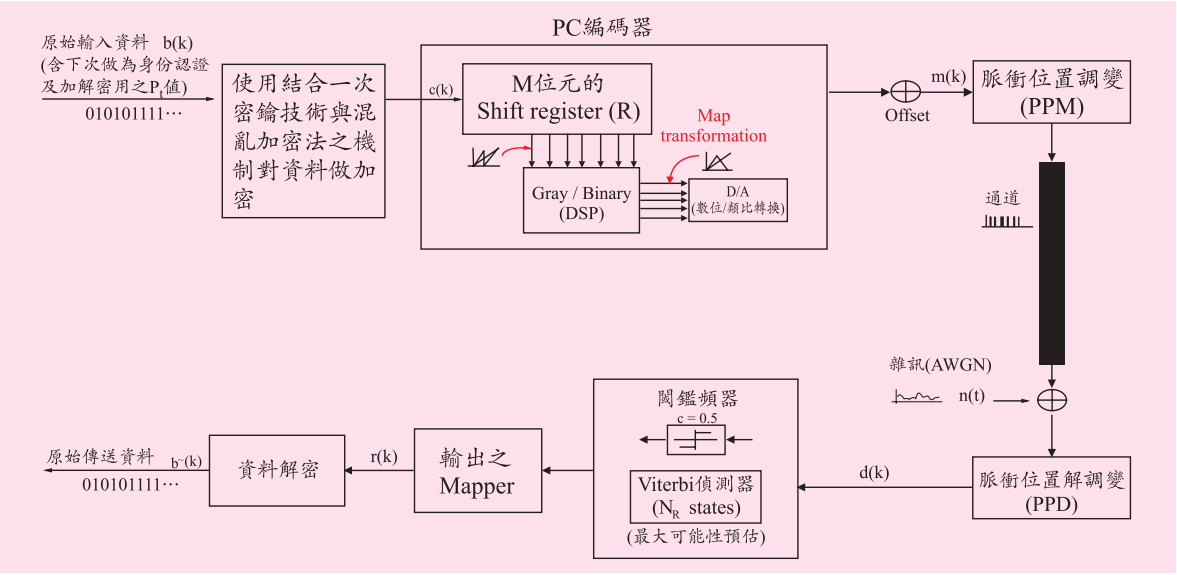
四、將欲傳送之資料，以三所述之方式將其轉化爲M位元的密文資料，同時並將OSPA下次做爲身份認證的$a_{n+1}$值併在傳送資料中，送至接收端儲存，以做爲下次身份認證及資料解密之用。

五、將此一次密鑰結合混亂加密法的機制，取代圖二中的「資料壓縮及擾亂」步驟，並把做爲下次身份認證及資料解密之用的$a_{n+1}$值併入欲傳送之資料中（如圖七），便爲本文所提出之「結合混亂編碼與一次密鑰技術運用在超寬頻系統之模型」。

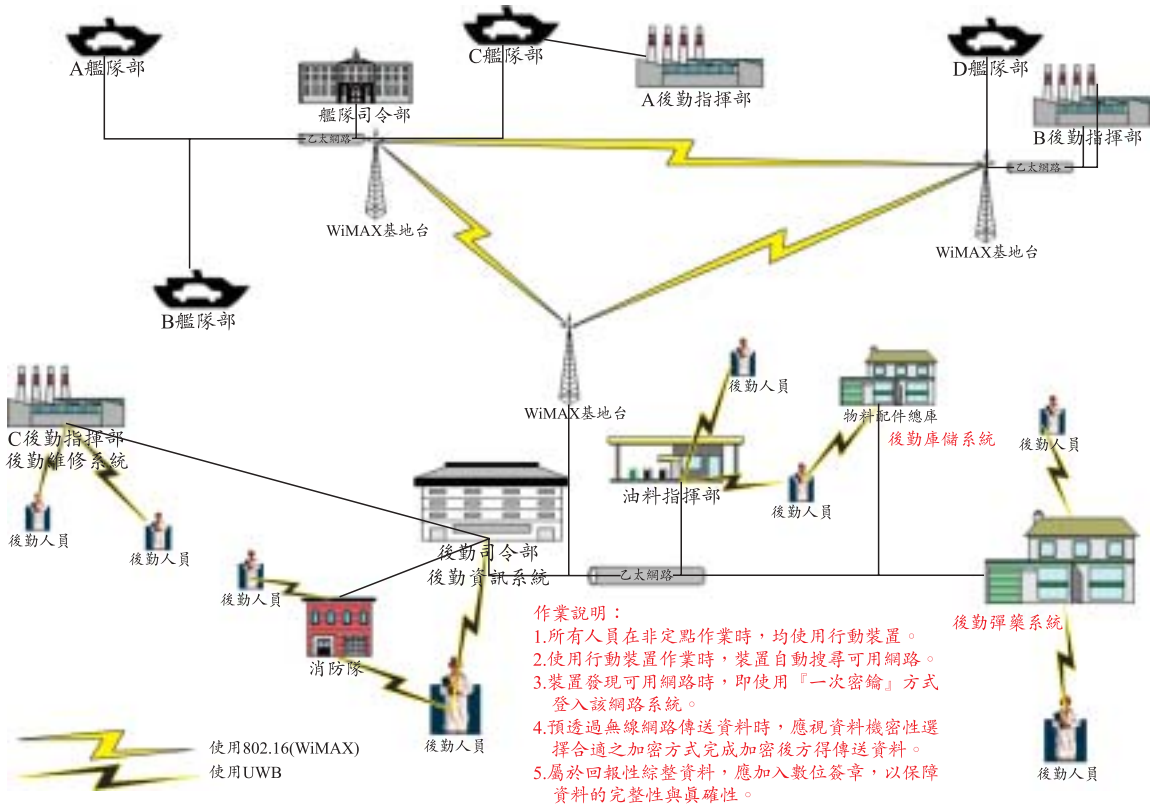
## 無線傳輸環境之設計

在此我們以UWB技術爲核心，運用前面章節所敘述之技術，設計一適合海軍單位使用的無線網路環境（如圖八），在圖八中，我們設計的無線網路環境架構大致上可分爲用在短距離傳輸的UWB技術，及傳輸距離較長的802.16(WiMAX)協定，搭配上海軍原本已建置完成的有線（固網）系統，便可形成一整合性的網路傳輸環境。

也就是說，藉由這樣的一個無線網路環境的實現，未來不管是艦艇戰鬥人員，或是艦艇的後勤維修人員，均可以無線傳輸裝置(PDA或是Notebook)，透過UWB或WiMAX等無線網路系統，完成各項作業。例如，在艦艇提出維修申請需求時，後勤維修人員便可




圖七　結合混亂編碼與一次密鑰技術運用在超寬頻系統之模型



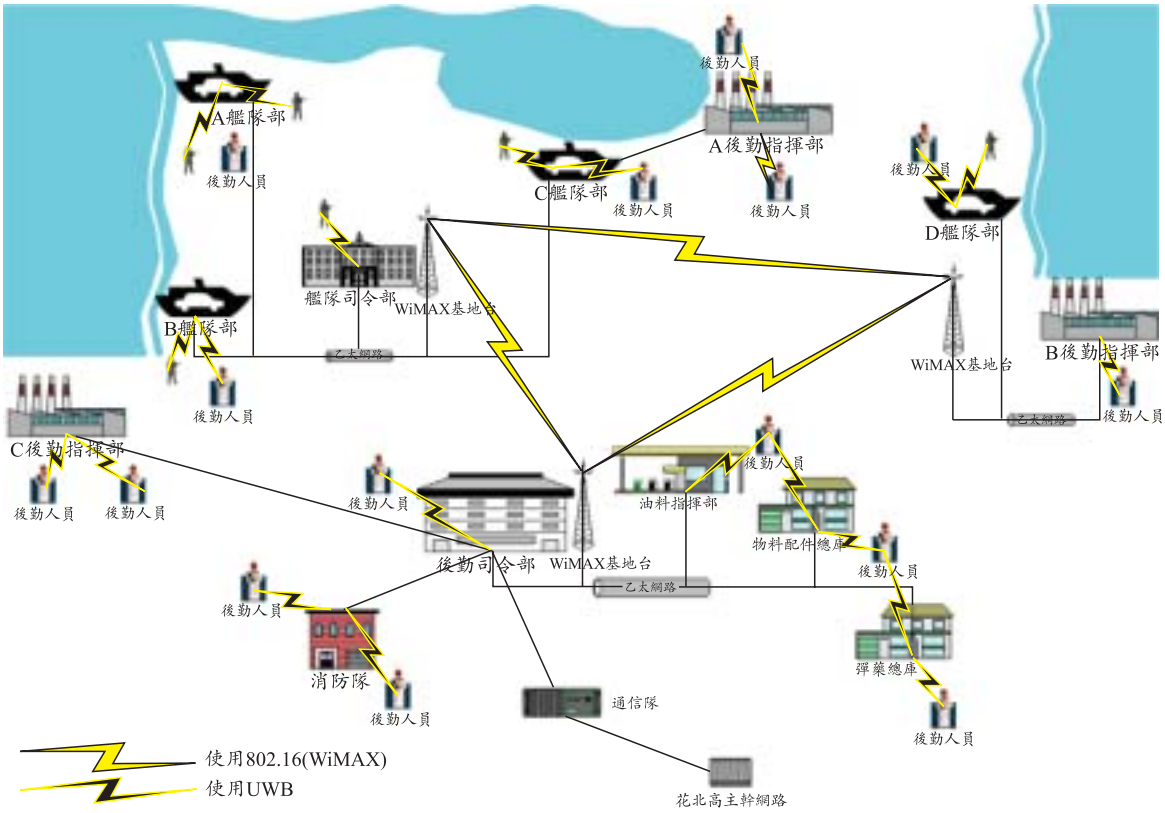

圖八　符合海軍作業需求之無線網路環境架構圖

攜帶PDA等無線裝置至艦艇上，透過UWB系統連上海軍的後勤系統，即時的查詢維修技令、各項物料庫存狀況，並即時反應艦艇維修需求至後勤系統中，不需再像之前的作業，需先派員勘查艦艇損壞狀況，再返回後勤部門查詢目前的物料庫存狀況及艦艇的排修狀況，才能決定是否需要備料或採購欠缺之物料，確實達到通訊及資訊之功能整合。而戰鬥或值勤人員，也可隨時透過無線裝置查詢艦艇各部門的狀況、即時反應各個部門的現況（例如巡察的危安狀況、各部門器材、人員的妥善狀況）、協調安排維修期程、任務特性等等。

此外，使用本研究所提出之機制，除可具有UWB的高速傳輸速度、高使用者容量及低訊號攔截率之優點外，因傳送的資料經過混亂加密結合計數式一次密鑰技術的加密，除非能破解出每次用來加密均不同的key值($P_t$)，並破解具有m!可能的資料組合方式，否則是不可能將加過密的資料還原成原始的狀態。綜合了以上的優點，再結合國軍現有之有線網路環境，便可形成一個整合型的網路環境架構（如圖九），而藉由此一整合型的網路，相信未來不管是在部隊或是機關單位，不論是使用有線網路或是無線傳輸，均能使國軍單位內各項有關資訊傳輸之安全性達到要求。

## 結論

UWB技術是近年來興起的幾項非常重要的無線傳輸技術之一，它與Blue Tooth技術相似，均是用在短距離傳輸的一項技術，




圖九　海軍整合型網路環境架構圖

但它具有極高速的傳輸速度（100M以上)、高容量、低耗電率及低攔截率等多項優點，且其成本相對於其他無線技術（例如WLAN）來說算是非常的低，因此其發展潛力可見一斑。

本研究係以可運用在UWB技術的PCTH技術爲基礎，透過該技術的資料傳輸機制，以結合一次密鑰技術與混亂加密技術的方法，來將傳送資料加密成符合PCTH機制要求的資料長度(M Bits)。藉由這樣的加密方式，不但能使傳送資料轉化爲符合長度要求的二元資訊，且因使用了一次密鑰技術與混亂加密方法，讓該傳送資料能具有極難被破解及僞冒的高安全性，這對需維持高機密性的國軍單位而言，更是具有重大的意義。因此，本文即以此爲出發點，研究將該技術運用在國軍任務特性上的可行性。而本文所提的「符合海軍單位使用之無線網路環境架構圖」，即是以本軍的任務特性爲背景所提出的一項供國軍未來無線網路環境佈建時的參考模型，運用此一特性，希能達到國軍在無線通訊上對資訊安全之要求。

## 作者簡介

江宗慶上尉，中正理工學院58期兵器系、國防大學國防管理學院國防資訊所94年班，曾任資訊官、資訊工程官，現任海軍基隆後勤支援指揮部計畫處資訊科程式設計官。

伍台國所長，美國佛羅里達大學資訊科學博士，現任國防大學國防管理學院國防資訊所所長。

陳正鎔助理教授，國防管理學院資源管理研究所碩士，現任職於萬能科技大學。