無線通訊安全

孫宏民、林岳勳

國立清華大學資訊工程系
Email: hmsun@cs.nthu.edu.tw

摘要

無線網路的最大的優點就是跨越了空間的限制，但這也是其缺點。以目前的有線網路來看，攻擊者想要擷取網路內部資料，必須進到網路內部。但在無線網路中，攻擊者並不需要實際進到網路內部；只要在無線網路可涵蓋的範圍內架設監聽器，例如建築物旁，就可以擷取到內部的無線網路傳輸資料了。所以在建置無線網路時，無線傳輸的安全性也需要考慮。本文中探討目前無線通訊上的安全技術，爲了涵蓋大部分的領域，我們根據媒介的不同來分別介紹。總共分成五個部分來探討無線通訊的安全技術：無線區域網路、點對點無線網路、行動電話、藍芽、無線感測器網路等。

關鍵詞：無線區域網路安全(Wireless Local Network Security)、行動電話系統安全(GSM Security)、點對點無線網路安全(Ad Hoc Network Security)、藍芽(Bluetooth)、無線感測器網路(Wireless Sensor Network)、公開金鑰系統(Public Key Cryptography)、無線通訊安全(Wireless Communication Security)

一、前言

無線通訊技術在最近幾年如雨後春筍般蓬勃發展。估計到公元 2006 年時，無線市場值會突破 2.7 百萬美元產值[15]。無線通訊現在已經不是新的名詞，而是一個非常普及的技術。從你使用的行動電話、藍芽裝置或手提電腦的無線網路卡，無線通訊無所不在。

無線網路的最大的優點就是跨越了空間的限制，但這也是其缺點[14]。以目前的有線網路來看，攻擊者想要擷取網路內部資料，必須進到網路內部。原則上必須先跨過防火牆及入侵偵測系統等。若是攻擊一個封閉網路，攻擊者更必須利用實體網路線連接上內部網路後，才可能擷取內部網路傳輸中的資料。但在無線

網路中，攻擊者並不需要實際進到網路內部；只要在無線網路可涵蓋的範圍內架設監聽器，例如建築物旁，就可能擷取到無線網路內部傳輸的資料了。所以在建置無線網路時，無線傳輸的安全性也需要同時考慮。

本文主要探討目前無線通訊上的安全技術，為了涵蓋大部分的領域，我們根據媒介的不同分別加以介紹。總共分成五個部分來探討無線通訊的安全技術：

(i)無線區域網路(Wireless Local Network, WLAN)。

(ii)點對點無線網路(Ad Hoc Network)。

(iii)行動電話(GSM, 3G)。

(iv)藍芽(Bluetooth)。

(v)無線感測器網路(Wireless Sensor Network, WSN)。

二、無線區域網路安全

無線區域網路大概是無線通訊最炙手可熱的，也是應用最廣泛的。WLAN 大家都耳熟能詳，它主要是遵循 802.11 標準。

(一) 802.11 是如何運作？

首先我們先了解 802.11 如何運作。無線網路利用無線電來傳輸資訊。所有無線電裝置利用不同的頻帶，在不互相干擾下進行傳輸。802.11 主要是利用 ISM 頻帶。原先一開始 802.11 標準是使用 900 MHz 頻帶，不過由於 ISM 頻帶是 2.4GHz，所以 802.11b 和 802.11g 使用 2.4 GHz 頻帶，而 802.11a 則使用 5 GHz 頻帶。這些頻帶是和一些電器分享的，像是微波爐和無線電話，所以會造成干擾。不過使用 ISM 頻帶也有其優點，因為使用 ISM 頻帶不需要申請執照。

(二)802.11 標準

即使在 WLAN 上有很多其他標準協定，不過最常在工業上使用的還是 802.11 和 Wi-Fi (Wireless Fidelty)。802.11 標準是由國際電子電機工程師學會(Institute of Electrical and Electronics Engineers, IEEE)[27]發展出來，並在 1997 公布發行。目

前，在 IEEE 有一組的委員會負責制定 802.11 相關標準。每一個小組用一個字母標示其所發展的標準，像是 802.11a 或 802.11b。表 1 是目前 IEEE 在推動 802.11 相關的歷史和目前的活動情形[27]。

另一個 WLAN 標準是 Wi-Fi [35]，Wi-Fi 聯盟是一個非營利組織，成立於 1999 年，主要的工作是認證 WLAN 產品是否有遵循 IEEE 802.11 標準。目前負責認證產品是否有遵循 802.11a/b/g 標準。另外，Wi-Fi 聯盟開始提供對熱點(Hot Spot)的認證，稱為 Wi-Fi 區域(Wi-Fi Zone)。想成為合格的 Wi-Fi 區域，熱點需使用擁有 Wi-Fi 認證的產品，且提供 VPN 的服務才行。

表 1　802.11 任務群組制定標準活動

標準	制定	頻帶	傳輸速度	調變方式	備註
802.11	1997	900 MHz	2 Mbps	FHSS	已廢棄不用。
802.11a	1999	5 GHz	最大 54 Mbps	OFDM	低傳輸距離、高傳輸率。
802.11b	1999	2.4 GHz	1-11 Mbps	DSSS	提升 802.11 傳輸速度到 2 Mbps。
802.11g	2003	2.4 GHz	最大 54 Mbps	OFDM	高傳輸率，和 802.11b 的規格相容。
802.11d	著重在延伸無線技術到 IEEE 無法涵蓋到的國家。				
802.11e	著重在改善多媒體上的傳輸及服務品質。				
802.11f	著重在加強在無線網路基地台之間的漫遊和廠商間的互通性。				
802.11h	著重在制定 5GHz 的動態頻率選擇(Dynamic Frequency Selection)技術及能源控管機制(Power Control Mechanism)。				
802.11i	著重在加強安全性，內容包含改善金鑰分佈方法和一些進階加密技術。				

(三) 802.11 安全標準

我們首先來檢視 WLAN 上的一些公開的安全標準，這一個部分包含了 WEP 和 802.11i 等公用標準。其次討論在有線網路上的既有安全機制，移植到 WLAN 上實作的情況，最後則是討論未來的方向及所面臨的挑戰。

(1)WEP

802.11 標準已經有內建有線等效加密法(Wired Equivalent Privacy, WEP)。不

過 WEP 已經被證明是不安全的，有多項安全性弱點[8]。大部分的無線網路裝置都有內建 WEP，不過為了安全性的關係大都是預設關閉。一但 WEP 啟用，網路駭客就可以輕易的破解它。AirSnort[16]就是一個網路上可以免費下載的 WEP 破解工具。因為 WEP 是 802.11 標準的一部分，所以一般建議還是應該開啓 WEP，雖然 WEP 僅提供最低的安全性，不過它還是可以減緩駭客攻擊的速度[29]。

(2)802.11i

802.11i[6]草案在 2004 年 6 月 24 日核准公布，用以取代先前被證實有多項安全漏洞的 WEP。802.11i 協定主要分成兩個層次。較低的那一層是定義加密演算法，包含改善 WEP 加密演算法部分，其中包含暫時金鑰完整性協定(Temporal Key Integrity Protocol, TKIP)及計數器模式(Counter Mode)的具有 CBC-MAC 協定(CBC-MAC Protocol, CCMP)的高級加密標準(Advanced Encryption Standard, AES)。TKIP 用在較舊的 WLAN 設備上，而 CCMP 是用於較新的 WLAN 設備上。另外，上層則是加密層，使用了 IEEE 802.1x 標準。

(3)密碼保護

密碼(Password)是認證上最簡單的一種方法。密碼通常是由一些容易記憶的字母、數字或符號所組成。當然，密碼必須由管理者及使用者雙方知道。不論是使用暴力法(Brute Force)，複雜的猜測機制或是去存取儲存密碼的檔案，駭客可以利用上述方法通過密碼的測試。不過一個良好的密碼可以讓駭客付出比較多的時間去破解它[30]。

(4)Kerberos

Kerberos[2]可以安全的認證使用者是否可存取網路。使用者連結到伺服器去取得數位憑證(Digital Certificate)和一把加密使用的金鑰，還有一把交易金鑰(Session Key)。交易金鑰是用在要求網路服務時，而數位憑證在協定中主要的功能是讓服務可以認證正在使用的使用者身份。至於資料串流的完整性則是利用標準資料加密法(Data Encryption Standard, DES) [7]。

(5)RADIUS

RADIUS (Remote Authentication Dial-In User Service) [19]是一個 AAA 協定，也就是對於遠端存取的連線進行認證、授權和計費等三種服務的協定。當使用者

登入時必須輸入他的使用者名稱及密碼給 RADIUS 伺服器。RADIUS 伺服器決定使用者是否有授權使用網路。它可以設定成對網路提供不同的存取層級。在使用者和 RADIUS 伺服器之間的通訊是加密保護的。然而，RADIUS 協定不提供資料加密。而且 RADIUS 經常和 VPN 一起使用。

(6)Diameter

由於 RADIUS 本身有些缺點，IETF[28]的 AAA 工作小組後來設計了 Diameter 協定[32]，用來取代 RADIUS 作為下一代的 AAA 協定標準。Diameter 是直徑的意思，意味着 Diameter 協定是 RADIUS 協定的升級版本。Diameter 協定包括：基本協定、網路存取協定(Network Access Service, NAS)、擴增式認證協定(Extensible Authentication Protocol, EAP)、行動 IP 協定(MIP)、密碼學訊息語法協定(Cryptographic Message Syntax)等。

另外，Diameter 協定支持行動 IP、NAS 請求和行動代理的認證、授權和計費工作。實作和 RADIUS 相似，但是內容中詳細規定了錯誤處理機制、不中斷機制(Failover Mechanism)，採用 TCP 協定，支持分散式計費，克服了 RADIUS 的許多缺點，是最適合未來行動通信系統的 AAA 協定。

(7)公開金鑰基礎建設

公開金鑰基礎建設(Public Key Infrastructure, PKI) [31]是一個可以用來提供公開金鑰密碼系統服務的整合套件。在密碼學上，公開金鑰密碼系統因為它使用的金鑰是一對的，包含公鑰及私鑰，所以也稱為非對稱金鑰。公開金鑰的擁有者把私鑰當成秘密保存，而把公鑰公開給其他人使用。私鑰及公鑰加密的密文，可以用另一金鑰解密。舉例來說，通常私鑰是用來加密訊息和簽章，而公鑰則是用來解密和驗證私鑰所簽的簽章。在安全網路交易和虛擬私有網路上，PKI 是很重要的基礎技術。

(8)虛擬私有網路

虛擬私有網路(Virtual Private Network, VPN) [32]提供一個虛擬的通道，允許使用者透過網際網路去存取公司的內部網路。它包含了認證、加密和封裝資料方法。架設 VPN 有很多種方式，不過有些是非常昂貴的。為了提供一個安全的環

境，網路管理者必須小心地設定 VPN。通常會利用 VPN 的情況是使用者在傳遞訊息時，需要最高等級的安全性；不過，相對應的是 VPN 通常會降低網路效能。要改善 VPN 效能的現有的做法是尋求例如硬體加速的做法或是把演算碼直接實作成硬體處理器晶片。

(9)TKIP

暫時金鑰完整性協定(Temporal Key Integrity Protocol, TKIP)[17]是一個可以快速更新金鑰的協定(Rekeying Protocol)，大約每傳遞 10,000 個封包會產生一把新的金鑰。它的優點是不但可以彌補 WEP 演算法的不足，也可以向下相容目前市面上使用 WEP 的 802.11 產品。

(10)AES

高級加密標準(Advanced Encryption Standard, AES)[9]目前最新的對稱性加密技術。IEEE 想把 AES 設計到 802.11i 安全協定中，當成是標準的一部分。不過 AES 並沒有和過去的 802.11 產品有相容性，原因是因為在加解密上需要消耗較多的能源[13]，直接影響到效能的表現。

(11)WPA

Wi-Fi 聯盟有發展一套安全協定為 Wi-Fi 保護存取(Wi-Fi Protected Access, WPA) [17]。它利用 802.1x 進行認證和加密協定 TKIP，其中 TKIP 提供快速的重新更新金鑰(Re-keying)協定，它還提供了改善 WEP 的演算法。另外，WPA 加入訊息完整碼(Message Integrity Code, MIC)，它利用密碼學 checksum 抵擋了 forgery。傳輸者在它加密和傳送之前，會先 MIC 加到封包中並傳遞。接收端則利用 MIC 去檢驗此封包的正確性。若收到的 MIC 和算出來的 MIC 不一樣，則會丟棄這個封包。由於在 WPA 是屬於臨時修正 WEP 的過渡期的產品，之後又推出了 WPA2 為一完整的安全性套件。

(12)WPA2

在 2004 年 6 月，IEEE802.11i 制定出來之後。Wi-Fi 聯盟經過修訂後重新推出了具有與 IEEE802.11i 標準相同功能的 WPA2。Wi-Fi 聯盟表示 WPA2 是使用較安全的加密演算法 AES，可以滿足部分企業和政府機構等需要導入 AES 的用戶需求。在這裡我們列了一個比較表來比較 WPA 和 WPA2，如表 2 所示。

表 2　WPA 和 WPA2 的比較表

	WEP	TKIP	AES	IEEE802.1x
概要	無線區域網路中的普通加密方式。存在容易被破解的缺點。	加密用的隨機數長度比 WEP 增加了 1 倍。不易被破解。	功能强大的加密方式，2002 年 10 月美國政府已將其作爲標準採用。	對通過無線區域網路連線進行認證的方式。用於企業級產品。
WPA	○	○	—	○*
WPA2	○	○	○	○*

說明：＊表示有些產品不支援。

(13)802.1x 通訊埠基網路存取控制

802.1x[26]是 IEEE 發布的一個安全協定，它是前面提到的 802.11i 的上層協定。主要提供一個較安全的使用者認證和中央控管的安全模式。它限制使用者存取網路，除非是經由認證的使用者，其他人不可以使用網路。802.1x 提供對 WEP 金鑰管理的修正改善，不過只有認證的部分，並沒有改善加解密的演算法。不過由於它只提供單方向認證，所以會和 WEP 遭受到同樣的問題，例如連線截奪(Session Hijacking)，中間人攻擊(Man-in-the-Middle Attack)等。

以上我們分別簡介無線區域網路的安全技術，因為有 IEEE 努力建立新的標準，所以安全的機制很健全。

三、點對點網路的安全性

(一)什麼是點對點網路？

點對點網路(ad hoc Networking) [11]是一種無線區域網路的網路架構，有些類似所謂的點對點架構(Peer to Peer Architecture, P2P)。其為網路卡直接連接的方式，效率較高。但在一般的無線電網路架構上其實很少見，因為大多數的家用或辦公室的網路環境現在都少不了對網際網路的需求，有線與無線的網路相互連接已經是一種必要性了，大部分的工作環境都會架設存取點。

不過有些情形你會用的到這類的網路，假如您的工作需要到處發表簡報，帶著筆記型電腦及投影機，在現場使用無線網路以點對點將筆記型電腦與投影機連結使用，將非常便利。現在許多新款的投影機均有內建網路卡，並且可以搭配無線電網卡使用，支援 Ad-Hoc 連接的工作模式。

(二)點對點網路的安全性

由於點對點網路沒有固定的網路架構，整個網路都在空氣中完成建構。所有的裝置僅透過無線連結去建立網路，沒有所謂的中央控管機構。個別的裝置不僅和別人溝通，還擔任路由的工作，替鄰近節點傳送封包。因為網路拓樸的不固定性，易於遭受攻擊，其安全性機制是很難設計且複雜的。我們針對下面幾項作分析。

(1) 可利用性

在點對點網路中，保證網路可以使用比傳統的安全性重要多了。由於每個在網路中的裝置都得依賴其他裝置傳送封包到更遠的地方，很容易發生阻斷服務攻擊(Denial of Service Attack, DoS)。另外，由於資訊都在空氣中傳播，使得阻斷服務攻擊更容易。舉例來說，攻擊者可能利用大量封包去阻塞整個服務頻寬，亦或是利用強力無線電波干擾原本可用的頻段。另一種可能的做法是在網路中去傳送不正確的資訊來擾亂正常路由協定。路由在點對點網路中是一項重大的弱點。由於網路拓樸經常變動，路由須時時刻刻的維護，這也給了攻擊者很好的機會攻擊。當然在之後的文獻中也提到如何在攻擊下維持路由的正常。

另一個弱點是裝置的能源。當然，少數是有固定電源支援，不過大部分情形下，裝置是靠電池供應電源。在這種情形下，裝置會採取一些省電的措施策略，大部分是使裝置進入休眠狀態。而攻擊者若利用阻斷服務攻擊，就可以大量的消耗使用者的裝置電源，達到攻擊的效果。

(2)授權和金鑰管理

授權在點對點網路也是一個挑戰。很多原先可以使用的認證機制都會有問題。例如說須有第三者存在的策略或是基於身分的金鑰管理等。

然而，點對點網路或許可以提供一個良好的認證機制的點對點網路。最簡單的做法是利用密碼進行認證，進而在執行金鑰交換的過程建立一把可以使用的金鑰[3]。例如一個密碼認證加上 Diffie-Hellman 金鑰交換，便可以達到某種程度上的安全需求。

(3) 私密性與完整性

私密性在點對點網路上也是極為脆弱的。在無線通訊的條件下，使用者可以直接監聽到未加密或加密的訊息。由於點對點網路中的節點並沒有事先分享私密金鑰，在金鑰建立前，可能會因為被監聽而破解此把金鑰。關於完整性，一樣是要先部署金鑰。所以說金鑰管理是點對點網路安全的基礎建設，實在不可或缺。

四、行動電話系統的安全性

(一)GSM Security

GSM 的全名為泛歐行動通訊系統(Global System for Mobile Communication)，是目前世上使用最普遍的手機通訊系統[23]。根據 2002 年 9 月相關報導指出，GSM 在世界上的無線市場占有率高達 69%。GSM 名稱源自於 Group Special Mobile (GSM)，在 1982 年由 CEPT (The European Conference of Post and Telecommunications Administrations)組成，目的是發展全歐洲標準手機電信系統，進而取代當時無法整合的手機系統。但當 GSM 服務在 1991 興起時，GSM 的縮寫就變成了目前電信通訊系統的縮寫。

(1)GSM 安全架構[24]

GSM 是無線通訊標準中使用最廣泛的。在 GSM 中，每一個用戶都可各自歸屬於一個本地系統，並擁有有一個全球唯一識別碼(International Mobile Subscriber Identity, IMSI)，並與本地系統(Home Location Register, HLR)之間共有一把認證密鑰(Authentication Key)。

GSM 的設計者希望系統的安全是在一個本地系統(HLR)的控制之下，當用戶漫遊進入另外一個外地系統(VLR)時，訊息會被送到本地系統要求回應以產生通

訊金鑰，用來作為資料、信號和聲音的私密編碼。這些來自本地系統的回應是由外地系統請求而得到，每次撥出或接收會使用一個回應值，在所有的回應值用完之後，外地系統必須再送出新的訊息，以得到另外不同的回應值。

每個系統經營者可以選擇自己的認證機制，此時每個用戶和本地系統(HLR)共同擁有一些資料。用戶的安全僅由用戶身份模組(Subscriber Identity Module, SIM)來保護，SIM 可從行動電話中取出。SIM 卡是以智慧卡為基礎的系統，其目的是防止攻擊者更改和增加另外的身分。

接下來我們將詳細敘述 GSM 的安全措施，有多項安全功能已經整合到 GSM 系統中來保護電話用戶的隱私，包含：

(i)對已註冊的電話用戶進行認證；

(ii)資料傳遞使用加密技術；

(iii)行動電話沒有 SIM 卡不能使用；

(iv)在 GSM 網路上不允許重複的 SIM 卡；

(v)安全儲存金鑰 KI。

(2) 認證機制

認證程序如下:

(i)行動電話(MS)傳送行動用戶之全球唯一識別碼(IMSI)到網路上。

(ii)網路接收此 IMSI，並尋找相對應這個 IMSI 的私密金鑰 KI。

(iii)網路產生 128 位元的隨機數值(RAND)，並透過無線媒介傳送到行動基地台。

(iv)行動基地台利用回傳的隨機數字和儲存在 SIM 卡中的私密 KI，經由 A3 演算法計算出回應值(SRES)。A3 是一種認證演算法，輸入是 RAND（128 位元）和 KI（128 位元），產生 32 位元的 SRES；簡單來說，它可以歸類成一種單向雜湊函數，雜湊函數有不可逆的特性，也就是無法利用輸出去恢復輸入。

(v)同時，網路利用相同演算法及相同輸入值計算相對應的 SRES。

(vi)MS 傳送計算後的 SRES 到網路上。

(vii)網路比對 SRES 來驗證使用者。

驗證的方法是基於電話用戶的 SIM 卡上和其本地系統分享的私密 KI。當電話用戶購買了 SIM 卡，KI 產生後會安全的寫入 SIM 中並存放一份備份到本地系統中。當一個新的 GSM 電話用戶第一次使用它的手機，他的 IMSI 會被傳送到網路上的儲存。之後，會有一個暫時用戶識別碼(TMSI)分配給這個電話用戶。 除非真的需要，為了安全性起見，IMSI 之後就很少傳送。這樣可以避免攻擊者利用竊聽使用者 IMSI 的方式來分辨是哪一個使用者。每一個 TMSI 會持續使用直到用戶離開這個區域，網路才會再分配一個新的 TMSI 給使用者。

(3) 加密部分

資訊加密分成下面幾個步驟：

(i)產生密文金鑰 KC

GSM 使用金鑰 KC 去保護暴露在空氣中的資料及訊號。一但使用者已經完成認證，經由網路取得的隨機值和從 SIM 卡中取得的金鑰 KI，會經過 A8 金鑰產生演算法產生一把加密金鑰 KC。當然，為了安全起見，A8 演算法也是儲存在 SIM 卡之中。使用 A8 演算法產生的 KC，會和 A5 演算法一起作用，去加解密資料。注意交易金鑰是利用手機中 SIM 卡產生的，行動基地台一樣能利用相同組合的 KI， RAND，和相同的演算法產生相同的金鑰去解密資料。

(ii)加密資料

初始一個加密過的通訊是藉由 GSM 網路發出加密模式要求。當使用者接受到此命令，便會開始加解密資料。每一個在空氣中傳遞的訊框會利用不同的金鑰串流(Key Stream)來加密資料，加密的演算法是 A5 演算法。A5 演算法是實作在手機硬體上，所以它可以在線上直接作加解密動作，以增加效能。

(4) 其他安全特性

智慧卡(Smart Card) [33]就像個微電腦一樣，擁有記憶體、中央處理器和簡單的作業系統。利用對唯讀記憶體程式化，它可以安全地存放一些隱密的資料。所以它可以提供比較好的方法來儲存 KI 和 IMSI 及其他私密資料。

(二)3G 上的安全性架構

3G 無線應用的安全性極為脆弱，在日本發生的惡意電子郵件入侵行動電話手機就是個明顯的例子，它會執行郵件所附的病毒程式，控制受感染的通訊裝置，某些時候還會不停打電話給日本緊急事故專線，更嚴重的是行動電話會完全當機，用戶再也無法使用電訊業者的服務。越來越多手機受到這類或其它的惡意攻擊，例如垃圾郵件、拒絕服務、病毒攻擊、盜取手機內容和惡意駭客入侵；毫無疑問的，過去十年來對桌上型電腦造成極大威脅的安全漏洞，現在正蔓延至無線通訊世界，包括行動電話、智慧型電話、PDA、膝上型電腦等無線通訊裝置。而要保護無線通訊裝置和使用這種傳輸媒介的應用，其困難程度也遠超過保護桌上型電腦的應用。不同於無線裝置，桌上型裝置只提供數目有限，而且可以辨識的對外連接點，廠商可對這些連接點進行嚴密的控制和保護。無線通訊則完全不同，重要資訊時常被置於行動裝置，很容易被竊取或遭受損害。

(三)3G 的認證協議

(1)3G 認證和密鑰分配協議

(a)協議過程

3G 系統的安全技術是在 GSM 的基礎上建立起來的，並充分考慮了和 GSM 系統的相容性。3G 系統沿用 GSM 的請求-響應認證模式，但是做了較大的改進。它通過在移動臺(MS)和歸屬環境／歸屬位置寄存器(HE/HLR)中共用的密鑰，實現 MS 和 HE/HLR 之間的雙向認證。

有三個實體參與 3G 認證與密鑰分配協議過程：MS、訪問位置寄存器／支援 GPRS 服務節點(VLR/SGSN)和 HE/HLR，具體步驟如下：

(i)當 MS 第一次入網或由於某種原因 VLR/SGSN 需要 MS 的永久身份認證時，MS 向 VLR/SGSN 發送用戶永久身份標識(IMSI)，請求註冊。在平時的認證中這一個步驟並不存在。

(ii)VLR/SGSN 把 IMSI 轉發到 HE/HLR，申請認證向量(AV)以對 MS 進行認證。

(iii)HE/HLR 生成 n 組 AV 發送給 VLR/SGSN。

其中，AV=n(RAND||XRES||CK||IK||AUTN)，這 5 個參數分別為隨機數(RAND)、期望響應值(XRES)、加密密鑰(CK)、完整性密鑰(KI)和認證令

牌(AUTN)。它們由如下的方法產生：

RAND 由 f0 產生

XRES=f2k(RAND)，

CK=f3k(RAND)，

IK=f4k(RAND)，

AUTN=SQN+(AAK||AMF||MAC)。

其中，SQN 是序列號；AK 是匿名密鑰，用於隱藏 SQN；AMF 是認證管理域；MAC 是消息認證碼。

AK=f5k(RAND)，

MAC=flk(SQN||RAND||AMF)。

f0～f5 是 3G 安全結構定義的口令演算法。f0 演算法只用在認證中產生隨機數，f1 演算法用於產生消息認證碼，f2 演算法用於在消息認證中計算期望響應值，f3 演算法用於產生加密密鑰，f4 演算法用於產生完整性密鑰，f5 演算法用於產生匿名密鑰。K 是 MS 和 HE/HLR 之間共用的密鑰。

(iv)VLR/SGSN 接收到認證向量後，將其中的 RAND 和 AUTN 發送給 MS 進行認證。

(v)MS 收到 RAND 和 AUTN 後，計算期望消息認證碼(XMAC)的值(XMAC=f1K(SQN||RAND||AMF))，並把計算結果和 AUTN 中的 MAC 比較，如不相等，則發送拒絕認證消息，放棄該過程。如果二者相等，MS 驗證 SQN 是否在正確的範圍內，若不在正確的範圍內，則 MS 向 VLR/SGSN 發送同步失敗消息，並放棄該過程。若上面的兩項驗證都通過，則 MS 分別計算響應值(RES，RES=f2k(RAND))，以及 CK、IK 的值，並將 RES 發送給 VLR/SGSN。

最後，VLR/SGSN 收到應答資訊後，比較 RES 和 XRES，相等則表示認證成功，否則表示認證失敗。

(b)安全性分析

該協議通過 MS 和 HE/HLR 共用的密鑰 K，實現了以下目標。

(i)MS 和 HE/HLR 之間的相互認證

VLR/SGSN 接收到來自 HE/HLR 的認證向量中包括了期望 MS 產生應答的 XRES(XRES=f2k(RAND))，如果 MS 是合法用戶，則 RES=XRES。而 MS 對 HE/HLR 的認證是通過 MAC 實現的。MS 接收到 VLR/SGSN 發過來的 MAC，計算 XMAC=f1k(SQN||RAND||AMF)，如果 MAC=XMAC，則表示認證成功。

(ii)MS 和 VLR/SGSN 之間的密鑰分配

VLR/SGSN 接收到來自 HE/HLR 的認證向量中包含的 CK1 和 IK1，合法用戶接收到正確的 RAND 之後，在 MS 中計算得到 CK2=f3k(RAND) 和 IK2=f4k(RAND)，並且 CK1=CK2，IK1=IK2。由於通信中的密鑰並沒有在空中傳輸，可確保密鑰的安全。

(c)可能的攻擊

通過上面的分析可以發現，3G 安全機制完全建立在 MS 和 HE/HLR 之間共用密鑰 K 的基礎之上，若該密鑰 K 洩漏，那麼通信中的安全將無從談起，攻擊者可以輕而易舉地在空中截獲 RAND，並用相關演算法取得相互認證且計算出 CK 和 IK，從而通信中的所有數據都可以被攻擊者截獲。由於這個密鑰 K 是長期不變的，所以一旦洩漏，將對用戶和網路營運商造成不可估量的損失。

(2)內容認證服務

國內安全電子商務服務供應商網際威信引進針對行動網路應用軟體的內容認證服務(Authenticated Content Signing, ACS)，期以透過建立相關程式發行者、下載內容的辨識性及有效性簽章，確保行動下載應用的安全性。

內容認證服務係由網路安全服務廠商 VeriSign 所發表的新一代程式簽章服務，提供行動應用程式開發者透過公正第三者認證的方式，做為該應用軟體在透過網路下載前的安全性確認，以避免使用者透過行動網路下載到內含有 bug，或不良意圖程式的應用軟體風險。

Verisign 的內容認證服務運作方式需由內容提供者先行申請發行者憑證(Publisher ID)及內容憑證(Content ID)，用以建立軟體或內容合法提供者的身份。

爾後，當內容提供者欲公開發表其內容或程式碼時，則須先將發行者憑證結合內容憑證傳送至 VeriSign 認證中心確認無誤後，再根據發行者的身份資料，以及應用程式的相關資訊亂數產出一組唯一的認證簽章。經重新認證簽章的內容會回傳給發行者，並以此認證內容開放公開下載。

(3)對於安全的考量

隨著數據傳輸的大量應用，對於網路安全的考量也日形重要。在 GSM 網路中，已採用了 3GPP 安全技術，3G 網路中，則尚有幾項重大修改。

(i)3G 的安全機制，將包含一些序列號碼，以供行動用戶與系統網路互相認證。

(ii)認證金鑰的長度增加，需要更強大的演算法則處理，整體加密更有保障。

(iii)3G 的安全機制是建立在交換機中，而不是像 GSM 一樣，建置在基地台上，因而可使得基地台與交換機之間的交換過程，亦能保障網路連結的安全性。

(iv) 3G 網路的通訊協定中，已內建有終端身份完整性機制(Integrity Mechanisms for the Terminal Identity, IMEI)，而 GSM 則是在之後才附加進去的。

五、藍芽上的安全性

(一)藍芽簡介

藍芽在無線通訊領域是一個新興的科技，它由一個 Bluetooth Special Interest Group (SIG)組織在 1998 年 3 月制定的。參與制定廠商分別有 Ericsson、Nokia、Intel、IBM 和 Toshiba 等大廠。之後，幾乎在電信業的大型廠商，像 3Com、Microsoft、Motorola 等都參與了 Bluetooth SIG 組織。目前參與的廠商已超過 1,500 家。 第一版的藍芽規範在 1999 年夏天公布，1.0B 版在 1999 的 11 月公布。而最新的第二版藍芽規範在 2004 年 8 月時公布[4]。

藍芽主要是用在短距離連結裝置。最常見的例子是無線連接行動電話到一台

個人數位助理(Personal Digital Assistant, PDA)或手提電腦上，而不用將行動電話透過其他介面連接；這具很大的便利性，也是藍芽之所以那麼流行的原因。藍芽也可以用於建立少數裝置(最多 8 個裝置)的點對點網路，叫做藍芽微網(Piconet)。這在數位會議上非常有用，所有的參與者都可以使用有藍芽裝置的手提電腦進行會議，並可以在使用者之間分享檔案。

(二)藍芽的安全性

在這一節中我們將詳細探討藍芽的安全性[21]。首先，在藍芽的安全機制上涵蓋幾個主要的元件，包含金鑰管理、加密和認證三個部分。

在每一個藍芽裝置中，皆有四個資訊用於維護連接層的安全性。第一個是藍芽裝置位址(Bluetooth Device Address, BD_ADDR)，是由 IEEE 所制定。它是一個 48 位元的位址，每一個藍芽裝置都有獨一無二的 BD_ADDR。私有認證金鑰(Private Authentication Key)，用於認證，是一個 128 位元的隨機值。私有加密金鑰(Private Encryption Key)，長度從 8 到 128 位元長度都有，主要用在加密。最後還儲存有一個隨機值(RAND)，長度 128 位元，由藍芽裝置自己產生的。

在藍芽的通用存取剖繪(Generic Access Profile)中，藍芽的安全機制被分成三個模式：

安全模式一：沒有任何安全性(Non-security)。

安全模式二：服務層的安全機制(Service Level Enforced Security)

安全模式三：連結層的安全機制(Link Level Enforced Security)。

模式二和模式三的差別是在模式三中藍芽裝置在建立通訊頻道之前就起動安全程序。而在裝置和服務上有不同的安全等級。對裝置而言，只有兩個層次，分別是信任裝置(Trusted Device)和不信任裝置(Untrusted Device)。信任裝置是指他擁有存取所有服務的權限，沒有任何限制。對服務而言，定義了三個安全性等級：需要認證及授權的服務，僅需要認證的服務和對所有裝置開放的服務。

(1)金鑰管理

所有在兩個或多個裝置中進行的安全過程都需要的連結層金鑰的支援。連結層金鑰的內容是一個 128 位元長度的隨機數。它主要的應用是在認證過程中，當

成參數產生加密金鑰。連結層金鑰的使用時間會根據它是暫時金鑰(Temporal Key)或是半永久金鑰(Semi-permanent Key)而不同。半永久金鑰可以在下次的認證時使用。而暫時金鑰只用在其中一次交易，不會重複使用。暫時金鑰通常使用在一對多的通訊上，也就是一份相同的資訊必須傳遞給多個接收者時。

在藍芽中，定義很多把不同種類的金鑰。連結金鑰(Link Key)根據不同型態的應用，可以是組合金鑰(Combination Key)、單元金鑰(Unit Key)、主金鑰(Master Key)或是初始金鑰(Initialization Key)，另外，它也適用於加密的金鑰。

單元金鑰是當單一裝置被安裝時所產生的金鑰。而組合金鑰則是當有兩個藍芽裝置必須互相交易時所產生的一對金鑰，是成對產生的。主金鑰是一把暫時性的金鑰，用來取代目前使用的連結金鑰。由於以藍芽建立的網路中，其中一個模式是所謂的主從模式，有一個主裝置。在這模式下，主金鑰可以在主裝置必須傳送給其他裝置時，用它加密。初始金鑰是用在當一開始時根本沒有組合金鑰或單元金鑰時使用的金鑰。不過它只用在初始階段。

在藍芽中使用的個人識別碼 (Personal Identification Number, PIN)，其長度可以從一到八個 8 位元組。在某些情況下四個位元的碼就足夠使用了，不過為了較高的安全性，必須使用更長的碼。PIN 碼在裝置中是固定的，所以當裝置要連結時必須輸入 PIN 碼。另一個可能輸入 PIN 碼是當兩個裝置在初始化時。

初始金鑰是在當兩個裝置沒有先前約定(Prior Engagement)卻需要溝通的情況下使用。在初始的過程中，兩個裝置必須輸入 PIN 碼。初始金鑰本身是利用 E22 演算法產生，如圖 1 所示。所產生 128 位元的初始金鑰是用在產生連結層金鑰的金鑰交換階段。當金鑰交換完成，初始金鑰就會被丟棄。

當第一次使用藍芽裝置時，利用 E21 金鑰產生演算法產生單元金鑰。這把金鑰一但被建立，就會儲存在不可揮發的記憶體中且很少更改。在初始化的過程中，應用程式會決定那一方必須提供它的單元金鑰當作是雙方的連結金鑰。若其中一方缺乏記憶體，像是無法記憶額外的金鑰，那就會使用它的單元金鑰當作連結金鑰。

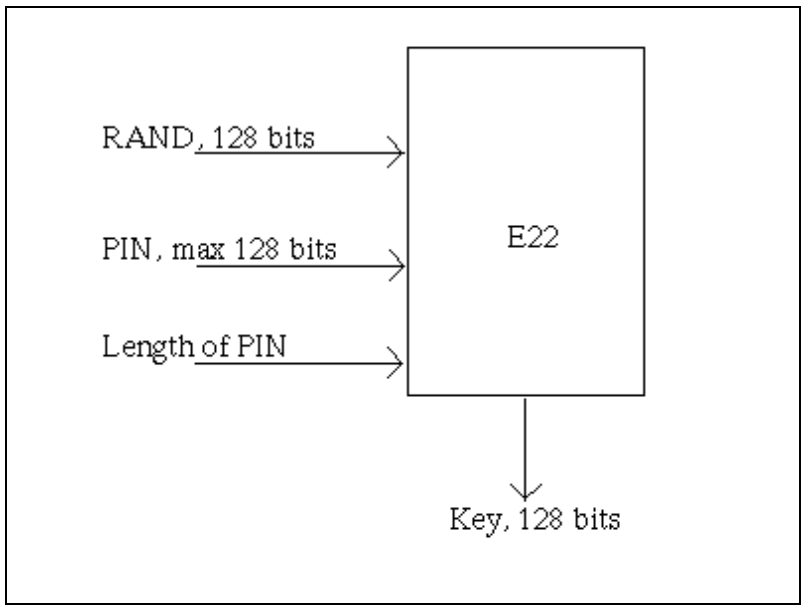

圖 1　E22 金鑰演算法

在初始過程中，當裝置決定需要組合金鑰會在這時候產生時。兩個裝置可以同時產生這把組合金鑰。首先，雙方會產生一個隨機值。利用金鑰產生演算法 E21，輸入則是結合隨機值和他們本身的藍芽裝置位址，來產生這把金鑰。

主金鑰是唯一的暫時性金鑰。在一群藍芽裝置中的主裝置，利用金鑰產生演算法 E22 和兩個 128 位元隨機值產生這把金鑰。由於 E22 演算法的輸出是 128 位元，因此所有的連結金鑰長度也都是 128 位元。接下來，第三個隨機值會傳到所有的次級裝置，並利用相同金鑰演算法，和目前所使用的連結金鑰，產生出一把新的連結金鑰。新的連結金鑰會傳送到次要裝置上，對重疊的部分逐位元進行 XOR 運算，則能算出主金鑰。這個過程能使主裝置和次要裝置都使用相同的主金鑰。

加密的金鑰是利用目前的連結金鑰和一個 96 位元長度的密文偏移數 (Ciphering Offset Number, COF)，以及一個 128 位元的隨機值一起產生，如圖 2 所示。密文偏移數乃是基於認證密文偏移值(Authenticated Ciphering Offset, ACO)，是在認證過程中產生。當連結管理程式(Link Manager, LM)啟動加密時，加密金鑰就產生了。不過加密金鑰在每次藍芽裝置進入加密模式時都會自動改變。

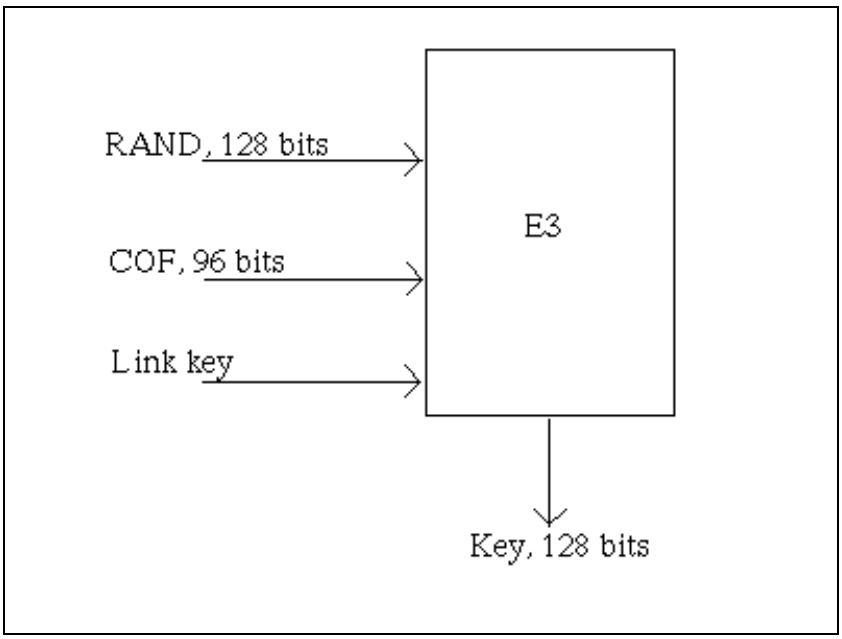

圖 2　E3 金鑰產生演算法

(2)加密機制

藍芽加密機制主要是用來加密封包的資料(Payload)部分。這可以利用 E0 串流加密演算法，可以將每一筆資料重新同步化。 E0 串流加密演算法包含加密資料用金鑰產生器(Payload Key Generator)、金鑰串流產生器(Key Stream Generator)和加解密演算法，由於其過程複雜，在 Saarinen M-J 所著「A Software Implementation of the BlueTooth Encryption Algorithm E0」書中可以找到更詳細的說明。

(3)認證機制

藍芽的認證機制使用兩回合挑戰-回應策略，雙方必須先分享一把密鑰，在兩回合或兩個步驟下，便可以完成認證程序。這個協定用的是對稱金鑰，成功的認證是基於雙邊都分享同一把金鑰。在認證過程中還會有項副產品，認證密文偏移值，會個別儲存在雙方藍芽裝置中，用於產生加密金鑰。

認證過程中，首先驗證者傳送一個隨機值進行認證要求。接著，雙方利用認證演算法 E1，把剛剛傳送的隨機值、被驗證者的藍芽裝置位置和目前使用的連結金鑰當成輸入，產生一個回應(SRES)。被驗證者會傳送回應給驗證者，進行比對之後，相同便表示認證通過，如圖 3 所示。

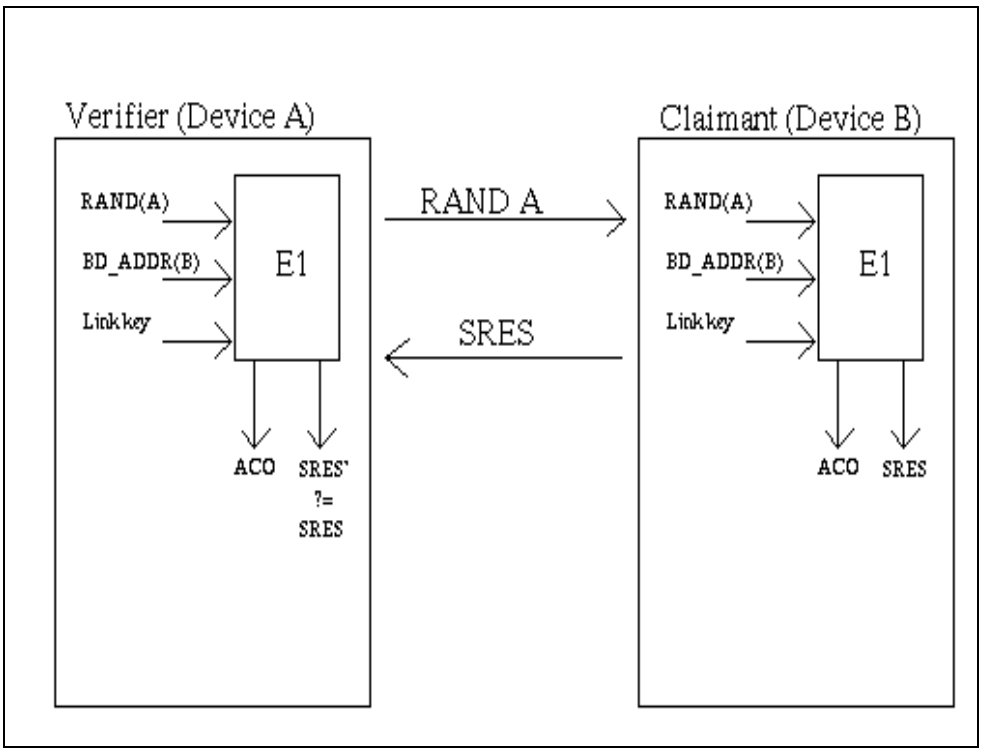

圖 3　認證演算法 E1

六、無線感測器網路安全性

(一)什麼是無線感測器網路？

由於近來微型製造技術、通訊技術及電池技術的改進，促使微小的感測器可具備有感應、無線通訊及處理資訊的能力[1]。感測器不但能夠感應及偵測環境的目標物及改變，並且可處理蒐集到的數據，並將處理過後的資料以無線傳輸的方式送到資料蒐集中心或基地台。

但是受限於感測器本身是用電池來供應運作所需的能量，以及無線電波傳輸的距離的限制（一般而言傳輸距離從數公尺到 100 公尺不等）。為了節省傳輸時的能量消耗及距離的問題，因此感測器如果距離基地台太遠時，感測器需要藉由多重跳躍代傳機制(Multiple-Hop Relay)建立路由的方法將資料經由多個感測器組成的路徑傳回基地台，此類感測器多為微小及便宜的裝置（由國外進口比較昂貴），因而可大量放置於環境中形成一個無線感測器網路(Wireless Sensor Network)以便進行監控任務，其放置的密度端看所需的應用為何，可大可小。由於感測器

網路的節點個數從數百至數十萬皆有可能，使得網路的管理非常困難，每個感測器都是獨立的個體，形成一個複雜的分散式環境，加上感測器的電池可能無法置換，因此能量控制幾乎是所有感測器設計及網路管理首要考慮的重點。再加上感測器為嵌入式系統裝置，它們故障的機會相形提高，因而容錯機制於感測器網路的設計及管理上亦不可或缺。

(二)無線感測器網路上安全機制

在發展無線感測器網路安全機制上最大的挑戰莫過於必須克服感測器本身的特性：能源限制及運算能力的不足。我們以美國加州大學柏克萊分校開發的微塵(Mote)當例子。Mote 僅有 4MHz 的處理器，128Kb 的隨機存取記憶體和 128Kb 程式記憶體空間，使用兩顆 AA 電池，封包的長度最大也只有 36 位元組。在這種限制下，使用公開金鑰系統(Public Key Cryptography)，或稱作非對稱金鑰系統；由於需要大量運算能源，所以對於無線感測器網路來說，要大量使用仍然是窒礙難行，很難達成的夢想。發展安全機制只能使用有效率的對稱式金鑰系統，不過封包的負擔仍然是一個很嚴重的問題。在傳統網路上，使用對稱式金鑰加密及認證機制，每一個封包至少需要 16 位元組。這在無線感測器網路上，已經佔了封包的一半長度。

由於無線感測器網路是一個新潮流，所以標準並不多，所以我們著重在已經是標準的 ZigBee(802.15.4)和美國加州大學柏克萊分校發展的感測器 Mote 使用的安全套件 TinySec。

(1)TinySec

我們首先介紹 TinySec[5]，它是一個在連結層加密的機制，主要是 TinyOS[34]的一個安全套件。最主要的部分是有效的區塊加密演算法和金鑰管理機制。TinySe 目前利用一把對稱式金鑰，由一群感測器分享。感測器在傳遞一個封包之前，首先會加密它的資料並附上此封包的訊息認證碼(Message Authentication Code, MAC)，通常是用密碼學上安全的雜湊函數來達成。當接收者收到封包時，可以利用 MAC 去檢驗這個封包是否有被竄改，接著可以將它解密。TinySec 擁

有最基本的幾個安全特性：存取權控制、訊息完整性和訊息隱密性。

(i)存取權控制和訊息完整性

存取權控制是指在連結層的節點必須防止未經授權的一方加入到合法網路中。合法的節點必須有能力去偵測從未經授權的節點傳送而來的封包，並且拒絕它。和訊息認證性很接近的是訊息認證性：如果攻擊者在傳輸資料過程中，修改從合法授權者傳來的訊息，那麼接收者必須有能力去辨識出資料已被竄改。TinySec 利用每個封包的訊息認證碼提供了訊息認證性及完整性。

(ii)訊息隱密性

隱密性是指對未授權的對象，能保持訊息的隱密性。通常是利用加密來達成這個特性。一個好的加密法不僅能避免訊息被還原回來，最好還能避免攻擊者利用加密過的密文中學習到某些部分的資訊。除此之外，加密最好要有所謂的語意安全(Semantic Security)，語意安全是指若有兩個明文經過加密產生兩個密文，在只給定其中一個密文的條件下，攻擊者沒有高於 50%機率可以正確猜對是由那一個明文所加密，因為純粹猜測的機率是一半。

(2)ZigBee

(a)什麼是 ZigBee？

ZigBee[34]這個字是指蜜蜂群跳一種像 ZigZag 形狀的舞蹈，這種舞有溝通作用的目的，因此作為新一代無線通訊技術之命名。ZigBee 之前叫做 HomeRF Lite、RF-EasyLink 或 FireFly 無線技術，目前稱為 ZigBee。

簡單來說，ZigBee 擁有下面優點：短距離、簡單架構、低能源消耗與低傳輸速率。傳輸距離約為數十公尺，使用頻段為免費的 2.4GHz 與 900MHz 頻段，和 802.11 使用的區段相同，傳輸速率從 20K 到 250Kbps。網路架構為主從式架構，可達到雙向通訊功用。

在標準規範之制訂方面，主要是 IEEE 802.15.4 小組[25]與 ZigBee 聯盟兩個組織負責，兩者分別制訂硬體與軟體標準，兩者之角色與分工就如同 IEEE 802.11

小組與 Wi-Fi 間的關係。在 IEEE 802.15.4 方面，2000 年 12 月 IEEE 成立了 802.15.4 小組，負責制訂媒體存取控制層(MAC)與物理層(PHY)，在 2003 年 5 月通過 802.15.4 標準。

802.15.4 任務小組目前則在著手制訂 802.15.4b 標準，主要是加強 802.15.4 標準，其包括：有解決標準疑義之處、降低複雜度、提高彈性並思考新的頻段分配等。

在 ZigBee 聯盟方面，ZigBee 聯盟是在 2002 年 10 月由一些大廠像 Honeywell、Mitsubishi、Motorola、Philips 與 Invensys 共同成立，到 2004 年 8 月約有 90 個會員。ZigBee 聯盟負責制訂網路層、安全管理、應用介面規範，其次亦肩負互通測試，預計在 2004 年底推出第 1.0 版。

(b)ZigBee 上的安全機制

802.15.4 規格中明確規定 ZigBee 上安全性是透過連結層安全機制達成，這一點和 TinySec 是一樣的。提供了連結層安全協定上最基本的四項安全服務：

(i)存取權控制：避免未經授權使用者存取網路。

(ii)訊息完整性：偵測訊息未經授權的修改。

(iii)訊息私密性：加密訊息可以限制監聽者了解訊息或明文，只有授權的合法者可以解密。

(iv)抵擋重送攻擊：避免攻擊者利用監聽取得的合法封包，重新傳送而認證成功。

在實作方面，安全套件定義了不同的 8 種安全演算法，不過大致上可以歸類為 4 種模式，如下：

(i)無安全性

(ii)僅加密(AES-CTR)

(iii)僅認證(AES-CBC-MAC)

(iv)加密與認證同時(AES-CCM)

詳細的內容請參考 Naveen Sastry 與 David Wagne 兩人在 2004 年 ACM Workshop on Wireless Security 中所提出論文「Security Considerations for IEEE

802.15.4 Networks」。認證是利用訊息認證碼(MAC)達成，為了提高彈性其定義三種不同長度的訊息認證碼，分別是 4/8/16 位元組。

七、結論

安全性在無線通訊上是一個非常重要的議題。從傳統的硬體接線到後來的空中傳播，潛在性的威脅愈來愈多，安全性似乎也相對應的越來越重要的。在本文中我們盡量涵蓋到所有無線通訊的範圍，包含了經常使用的無線區域網路和新穎的無線感測器網路，內容大都是著重於安全機制說明和安全協定。另外有些無法涵蓋到的部分，由於篇幅所限，也請讀者多多包涵。

參考文獻

1. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam, and E. Cayirci, A Survey on Sensor Networks, IEEE Communications Magazine, Aug. 2002, pp.102–114.

2. Amoroso E., Fundamentals of Computer Security Technology, Prentice Hall, 1994, p. 403.

3. Asokan N. and Ginzboorg P., Key Agreement in Ad-Hoc Networks, Feb. 23 2000.

4. Bluetooth SIG, Bluetooth Special Interest Group Launches Bluetooth Core Specification, Version 2.0 + Enhanced Data Rate, Press release, Nov. 8 2004.

5. Chris Karlof, Naveen Sastry, and David Wagne, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 2004.

6. Eaton, Dennis, Diving into the 802.11i Spec: A Tutorial, Nov. 26, 2002.

7. Eli Biham and Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.

8. Garfinkel, Simson, The Internet Amenity, Technology Review, Cambridge, Mar. 2002.

9. Joan Daemen and Vincent Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag, 2002.

10. Jon Edney and Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, 2003.

11. Kahn, R. E., The Organization of Computer Resources into a Packet Radio Network, IEEE Transactions on Communications, Vol. COM-25, No. 1, pp.169-178.

12. Naveen Sastry, and David Wagne, Security Considerations for IEEE 802.15.4 Networks, Wireless Security Proceedings of the 2004 ACM workshop on Wireless security, 2004.

13. Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting, Improved Cryptanalysis of Rijndael, Fast Software Encryption, 2000, pp213–230.

14. Stanley, Richard, Wireless LAN Risks and Vulnerabilities, Information Systems Control Journal, Vol. 2, 2002.

15. Superfast Wireless Heads to Homes: First Wireless G Products Hit the Market, Feb. 25, 2003.

16. Tanzella, Fred, Wireless LAN Security—How to Protect WLANs, Air Defense, Nov. 03, 2002.

17. Wi-Fi Alliance, Wi-Fi Protected Access: Strong, Standards-Based, Interoperable Security for Today’s Wi-Fi Networks, Retrieved Mar. 1 2004.

18. 3G Today, http://www.3gtoday.com/wps/portal/operators/.

19. AAA protocol, http://www.ietf.org/html.charters/aaa-charter.html.

20. Analysis of 3G Mobile Security, http://choices.cs.uiuc.edu/MobilSec/.

21. Bluetooth™ Security White Paper, http://www.bluetooth.com/upload/24Security_Paper.PDF.

22. Diameter, http://www.diameter.org/.

23. GSM Overview, http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html.

24. GSM Security FAQ, http://www.gsm-security.net/gsm-security-faq.shtml.

25. IEEE 802.15 WPAN™ Task Group 4, http://www.ieee802.org/15/pub/TG4.html.

26. IEEE on 802.1x, http://www.ieee802.org/1/pages/802.1x.html.

27. IEEE Standards Association, http://standards.ieee.org/faqs/wgdev.html.

28. IETF, The Internet Engineering Task Force, http://www.ietf.org/.

29. Karagiannis, Konstantino, Ten Steps to a Secure Wireless Network, Feb. 25, 2003, http://www.pcmag.com/article2/0,4149,844020,00.asp.

30. Password Crackers, http://www.pcmag.com/passwords.

31. PKI, http://www.pki-page.org/.

32. RFC 2764 -A Framework for IP Based Virtual Private Networks, http://www.ietf.org/rfc/rfc2764.txt.

33. Smart Card Alliance, http://www.smartcardalliance.org/.

34. TinyOS, http://www.tinyos.net/.

35. Wi-Fi Alliance, http://www.weca.net/OpenSection/index.asp?noFlash=true.

36. ZigBee, http://www.zigbee.org/en/index.asp.