發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：92122111

※ 申請日期：92-08-12　　※IPC 分類：H04L7/00

壹、發明名稱：（中文/英文）

具有侵入偵測特徵之無線區域網路或大都會區域網路及相關方法
WIRELESS LOCAL OR METROPOLITAN AREA NETWORK WITH INTRUSION DETECTION FEATURES AND RELATED METHODS

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）
美商賀利實公司
HARRIS CORPORATION

代表人：（中文/英文）
史考特 T. 米昆
SCOTT T. MIKUEN

住居所或營業所地址：（中文/英文）
美國佛羅里達州美爾鉢市西那沙路1025號
1025 WEST NASA BOULEVARD, MELBOURNE, FL 32919, U.S.A.

國　籍：（中文/英文）
美國　　U.S.A.

參、發明人：（共 1 人）

姓　名：（中文/英文）
湯瑪士 杰 比爾哈斯
THOMAS JAY BILLHARTZ

住居所地址：（中文/英文）
美國佛羅里達州美爾鉢市波羅尼斯路2355號
2355 POLONIUS LANE, MELBOURNE, FLORIDA 32934, U.S.A.

國　籍：（中文/英文）
美國　　U.S.A.

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☑ 本案申請前已向下列國家（地區）申請專利：

1.美國；2002年08月12日；10/217,243

2.

3.

4.

5.

☑ 主張國際優先權(專利法第二十四條)：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1.美國；2002年08月12日；10/217,243

2.

3.

4.

5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明係關於無線區域網路或大都會區域網路，具體而言，本發明係關於具有侵入偵測特徵之無線區域網路或大都會區域網路及相關方法。

【先前技術】

無線網路已經過數年以來的持續發展。兩項特定實例是無線區域網路(LAN)及無線大都會區域網路(MAN)。例如，在基本服務集(basic service set；BSS)中，此類網路包含一或多個無線工作站(例如，配備無線網路介面(NIC)的膝上型電腦)，無線工作站經由射頻信號來與存取點或基地台(例如，伺服器)通信。基地台執行許多功能，同步處理和協調、轉遞廣播封包以及提供一介於無線LAN/MAN與一有線網路(例如，電話網路)之間的橋接。

在擴充服務集(extended service set；ESS)中，網路中包含多個基地台。另一方面，在某些無線LAN/MAN中，可能根本沒有基地台，而只有以互相對等通信方式接合的無線工作站。這種拓樸稱為獨立型基本服務集(independent basic service set；IBSS)，並且在IBSS中，通常會選擇該等無線工作站之一當做一所缺少之基地台的代理伺服器(proxy)。

或許，無線LAN/MAN普及的最重要原因為，由於此類網路不需要有線基礎設施，所以相當便宜且很容易部署。當然，無線LAN/MAN也有一些顯著的缺點，而在有線網路找

不到這些缺點。例如，因為此類無線LAN/MAN裝置非常普遍，所以成為駭客者很容易獲得此類裝置，而得以使用未授權的無線工作站(即，惡意的工作站)嘗試侵入網路及洩露網路安全性。再者，如果無線LAN/MAN彼此之間的運作範圍太接近，則可能會遭到其他網路侵入，並且導致網路遭到破壞，尤其是網路共用通用頻道時。

在所發展之用於制定無線LAN/MAN內通信規章中的最著名標準之一為，電機電子工程學會(Institute of Electrical and Electronic Engineers；IEEE) 1999年的802 LAN/MAN Standards Committee，標題為「IEEE Standards for Information Technology--Telecommunications and Information Systems--Local and Metropolitan Area Network--Specific Requirements--Part 11：Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications」，其內容以引用方式併入本文。除了提供無線通信協定以外，802.11標準也定義一種有線等效保密(wired equivalent privacy；WEP)演算法，用於防止無線信號被竊聽(eavesdropping)。具體而言，WEP提供介於工作站之間所傳送之訊息的加密處理及完整性檢查，以確保原來傳輸之訊息的完整性尚未被洩露。

雖然WEP演算法提供了某種網路安全性措施，但是不提供可能侵入網路的偵測或報告。只有最近才可取得此類侵入偵測系統。這些系統通常包含在想要侵入偵測的工作站上安裝的安全性監視軟體。此類軟體嘗試偵測侵入者的方

式為，監視並且記錄媒體存取控制(MAC)位址或網際網路通訊協定(IP)位址，以及比較該等位址與已知授權網路工作站的位址。另外，此類系統可觀測何時未啟用WEP。

侵入偵測系統的一項特定實例為WildPackets, Inc.的AiroPeek。AiroPeek依據網路中使用的ESS及BSS識別項(ESSID、BSSID)來搜尋未經授權的惡意工作站。即，會建立網路中使用的經授權ESSID及BSSID清單。接著使用一篩選程式(filter)來排除所有未經授權的工作站。建立該篩選程式的方式為，擷取正常網路流量並且判斷802.11訊框中相對應於ESSID或BSSID的資料偏移。AiroPeek還包括一依據訊框計數而觸發的警示。即，如果訊框計數超過零，就會觸發警示(即，如果偵測到來自惡意工作站的任何訊框，就會觸發警示)。另外，AiroPeek可經由電子郵件來提供警示通知，或藉由數據機撥接以將警示傳出系統(例如，傳出至傳呼機)。

儘管前面系統的進展，此類系統仍然無法偵測到某些對無線LAN/MAN的侵入。也就是說，例如，如果惡意工作站已獲得存取經授權位址及/或ID，則前面做法就無法偵測到惡意工作站侵入網路。

【發明內容】

鑑於＜先前技術＞所述，因此本發明的目的是提供一種具有侵入偵測特徵的無線LAN/MAN及其方法。

根據本發明之這項及其他目的、特徵及優點係藉由一種無線區域網路或大都會區域網路所提供，該無線區域網路

或大都會區域網路可包括：複數個工作站，用於在該等工作站之間傳輸資料；以及一監督站。該監督站可藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測未經授權週期期間發生之傳輸；以及據此產生一侵入警示。

具體而言，該等工作站可使用封包來傳輸資料，並且產生要連同每個封包一起傳輸的所屬完整性檢查值。就其本身而論，該監督站可進一步藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測不符合所屬資料封包之完整性檢查值；以及據此產生一侵入警示。另外，可經由一媒體存取控制(MAC)層來傳輸該等資料封包；以及該等工作站還可以連同每個資料封包一起傳輸一所屬MAC序號。因此，該監督站還可藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測是否有一工作站使用非連續MAC序號；以及據此產生一侵入警示。

另外，每個資料封包都可具有一相關的封包類型，所以該監督站還可藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測是否具有預先決定封包類型之封包衝突；以及據此產生一侵入警示。具體而言，該預先決定封包類型可包含下列至少一項：多個管理訊框封包(例如，鑑認封包、關聯性封包及信標封包)、控制訊框封包(例如，「要求傳送」(request to send；RTS)封包及「清除傳送」(clear to send；CTS))及資料訊框封包

。因此，具有預先決定封包類型之封包的衝突臨限值次數可能大於(例如)約三。此外，臨限值次數可能係以所監視之具有預先決定封包類型之封包總數的百分比為基礎。

每個工作站都具有一要連同所傳送之資料一起傳輸的MAC位址。就其本身而論，該監督站可進一步藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測相同MAC位址之衝突；以及據此產生一侵入警示。舉例而言，相同MAC位址之衝突臨限值次數可能大於(例如)約三。

另外，該無線網路可具有相關的至少一服務集識別項(ID)。因此，該監督站還可藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測該等相關之服務集ID；以及依據該等所偵測之服務集ID之一不同於該無線網路之該至少一服務集ID來產生一侵入警示。而且，該等複數個工作站可透過至少一頻道來傳輸資料；以及該監督站可偵測是否有不是源自於該等複數個工作站之一的工作站透過該至少一頻道進行傳輸，並且據此產生一侵入警示。

該監督站還可進一步將一侵入警示傳輸至該等複數個工作站中至少一工作站。另外，該監督站可能是基地台，並且可能是一無線工作站。

一種本發明之侵入偵測方法觀點係運用在包含複數個工作站的無線區域網路或大都會區域網路。具體而言，該方法可包括：該等工作站之間正在傳輸資料，並且監視該等

複數個工作站之間的傳輸，以便偵測未經授權週期期間發生之傳輸。另外，可依據在未經授權週期期間偵測到傳輸而產生一侵入警示。

此外，該等複數個工作站可使用封包來傳輸資料，並且產生要連同每個封包一起傳輸的所屬完整性檢查值。就其本身而論，該方法也可包括：監視該等複數個工作站之間的傳輸，以便偵測不符合所屬資料封包之完整性檢查值；以及據此產生一侵入警示。

可經由一媒體存取控制(MAC)層來傳輸該等資料封包；以及該等複數個工作站還可以連同每個資料封包一起傳輸一所屬MAC序號。因此，該方法還可包括：監視該等複數個工作站之間的傳輸，以便偵測是否有一工作站使用非連續MAC序號；以及據此產生一侵入警示。

每個資料封包還可具有一相關的封包類型。因此，該方法也可包括：監視該等複數個工作站之間的傳輸，以便偵測是否具有預先決定封包類型之封包衝突；以及依據偵測該具有預先決定封包類型之封包的衝突臨限值次數，而產生一侵入警示。舉例而言，該預先決定封包類型可包含下列至少一項：多個管理訊框封包(例如，鑑認封包、關聯性封包及信標封包)、控制訊框封包(例如，「要求傳送」(request to send；RTS)封包及「清除傳送」(clear to send；CTS))及資料訊框封包。另外，衝突的臨限值次數可能大於約三。此外，臨限值次數可能係以所監視之具有預先決定封包類型之封包總數的百分比為基礎。

該等複數個工作站可經由一MAC層來傳輸資料；以及每個工作站都具有一要連同所傳送之資料一起傳輸的MAC位址，如上文所述。因此，該方法可進一步包括：監視該等複數個工作站之間的傳輸，以便偵測相同MAC位址之衝突；以及依據偵測到一相同MAC位址的衝突臨限值次數來產生一侵入警示。舉例而言，衝突的臨限值次數可能大於約三。

該方法也可包括：監視該等複數個工作站之間的傳輸，以便偵測該等相關之服務集ID；以及依據該等所偵測之服務集ID之一不同於該無線網路之該至少一服務集ID來產生一侵入警示。而且，可偵測不是源自於該等複數個工作站之一的工作站透過該至少一頻道進行傳輸；以及可據此產生一侵入警示。還可將該侵入警示傳輸至該等複數個工作站中的至少一工作站。

【實施方式】

現在將參考用以呈現本發明較佳具體實施例的附圖來詳細說明本發明。然而，本發明可運用許多不同形式具體化，並且不應視為限於本文中提出的具體實施例。而且，提供這些具體實施例以徹底且完整發表本發明，並且將本發明的範疇完整傳達給熟知技藝人士。

基於前述討論之目的，整份說明書中相似的數字代表相似的元件。另外，特別在請參閱圖1至圖10時，會使用相差十的參考數字來標示替代具體實施例中的相似元件。例如，圖1至圖10中所標示的無線工作站11、21、31、41、51

、61、71、81、91及101都是想要的元件，以此類推。因此，只要在元件第一次出現時才會加以詳細說明，以避免不適當重複說明，但是應明白，之後出現的元件類似於第一次所說明的元件。

現在請參閱圖1，圖中所示之根據本發明的無線LAN/MAN 10包括一無線工作站11及一基地台(或存取點)12。雖然基於簡化圖式目的，圖中只有描繪出一單一無線工作站11及基地台12，旦是熟悉此項技術者應明白，無線網路10內可包含任何數量的無線工作站及/或基地台。

在詳細說明無線網路10之前，先提供關於無線LAN/MAN通信協定的簡短討論。具體而言，基於清楚解說之考量，前述的討論將呈現出使用802.11標準的網路實施。然而，熟知技藝人士應明白，本文中所說明的許多觀點及具體實施例也可配合其他適用的LAN/MAN標準(例如，藍芽等等)一起使用。

802.11標準運用在配合用於資料傳輸之包含七層的OSI網路模型一起使用，各層使用各種通信協定來傳送某些類型之資料。OSI網路模型的七層包括應用層(application layer)、表達層(presentation layer)、會期層(session layer)、傳輸層(transport layer)、網路層(network layer)、資料鏈路層(data link layer)及實體層(physical layer)。資料鏈路層進一步包括媒體存取控制(media access control；MAC)子層及邏輯鏈路控制(logical link control)子層。例如，具體而言，無線工作站11及基地台12之間使用MAC層來傳輸資料

，尤其無線工作站11及基地台12各有相關的MAC位址。當然，也可使用OSI網路模型來傳輸資料。另外，通常會以封包格式來傳送資料，並且會針對不同類型的訊息資料來使用各種封包類型，如下文中的詳細說明所述。

根據本發明，作為實例的無線網路10包含一監督站13，用於偵測一惡意工作站14對該無線網路之侵入。舉例而言，成為駭客者可能使用該惡意工作站14來嘗試侵入該無線網路10，或可能僅僅是來自極接收該無線網路10運作之不同無線網路的節點。該監督站13可包括一或多個無線工作站及/或基地台。在本實例中，該監督站13監視該等工作站11、12之間的傳輸，以便偵測來自一MAC位址的訊框檢查序列(FCS)錯誤。如果偵測到既定MAC位址的FCS錯誤數量超過一臨限值，則該監督站13據此產生一侵入警示。

請注意，在本文中使用的用詞「在工作站之間傳輸」預定表示工作站11、12之間的任何直接傳輸，以及在該無線網路10運作範圍內的任何傳輸。換言之，該監督站13都可監視導向至或源自於工作站11、12的傳輸以及可接收的任何其他傳輸，而無論是否是明確導向至或源自於該無線網路10內工作站的傳輸。

在如上文所述的具體實施例(及如下文所述的具體實施例)中，該監督站13可有利地將警示傳輸至該無線網路10內的一或多個工作站11、12。舉例而言，該監督站13可將侵入警示直接傳輸至基地台12，接著由該基地台12通知無線網路中的其他工作站。或者，該監督站13可將侵入警示廣

播至所有網路工作站。在任一情況下，接著可採取適當的對策來回應未經授權之侵入，如熟悉此項技術者所知。此類對策不屬於本發明範疇，因此本文中不會加以討論。

現在請參考圖2，現在說明第一項替代具體實施例之無線LAN/MAN 20。在本具體實施例中，該監督站23偵測對該無線網路20之侵入的方法為，監視該等工作站21、22之間的傳輸，以便偵測鑑認MAC位址的失敗嘗試。在偵測到鑑認一特定MAC位址的失敗嘗試預先決定次數之後，該監督站23將產生一侵入警示。

可使用任何失敗嘗試次數來當做用於產生侵入警示的臨限值，但是通常允許至少一次鑑認MAC位址嘗試，而不會產生侵入警示。另外，在某些具體實施例中，最佳方式為，該監督站23只有在一預先決定週期期間(例如，一小時、一天等等)發生偵測到失敗次數，才能產生侵入警示。

按照802.11標準，想要在無線LAN/MAN內互相通信的兩個工作站通常會在傳輸資料之前先在工作站之間傳輸「要求傳送」(request to send；RTS)封包及「清除傳送」(clear to send；CTS)封包。這是基於避免與其他傳輸發生衝突之原因。即，由於無線LAN/MAN中的許多或所有工作站可能會在相同頻道上通信，所以工作站必須確定不會同時進行傳輸，否則就會導致干擾及使網路瓦解。另外，該RTS封包及該CTS封包通常包括一網路配置向量(network allocation vector；NAV)，用於指示一為傳輸資料所保留的持續時間。這項資訊被傳輸至無線LAN/WAN中的所有其他

工作站，接著在特定週期期間停止傳輸。

現在請參閱圖3，現在說明第二項替代具體實施例之無線LAN/MAN 30，其中該監督站33偵測對該無線網路30之侵入的方法為，監視該等工作站31、32之間傳送的RTS封包及CTS封包，以便偵測該封包中的非法NAV值。例如，可實施該無線網路30的方式為，資料傳輸不可超過一段時間，這是參與之經授權工作站已知的時間。因此，如果該監督站33偵測到不屬於指定時間範圍內的NAV值，就會據此產生一侵入警示。

802.11標準的另一項特徵為，無線LAN/MAN內的工作站可在競爭模式及無競爭模式下運作。即，在競爭模式中，所有工作站都必須競爭存取特定頻道，才能傳輸資料封包。在無競爭週期(CFP)期間，由基地台控制媒體之使用，因此工作站不需要競爭頻道存取。

根據圖4所示之第三項具體實施例之無線LAN/MAN 40，其中該監督站43有利地偵測對該無線網路40之侵入的方法為，監視該等工作站41、42之間的傳輸，以便偵測非CFP期間的無競爭模式運作。據此，該監督站43以此類偵測為基礎而產生一侵入警示。換言之，偵測到一工作站在非CFP期間以無競爭模式運作，表示該工作站不是經授權工作站，因為當已開始CFP時，基地台42已通知所有經授權的無線工作站。當然，這也適用於圖5所示之具體實施例，其中會偵測CFP期間的競爭模式運作。熟知技藝人士應明白，可在一既定應用中實施如上文所述之CFP侵入偵測做法之

一或兩者。

現在請參考圖6，現在說明另一項具體實施例之無線LAN/MAN 60。在本具體實施例中，該監督站63偵測對該無線網路60之侵入的方法為，監視該等工作站61、62之間的傳輸，以便偵測未經授權期間的傳輸。即，可實施無線網路60，而得以在指定時刻(例如，半夜十二點鐘至早上6:00之間)不允許使用者存取網路。因此，在該未經授權期間偵測到傳輸之後，該監督站63可有利地產生一侵入警示。

現在請參考圖7，現在說明另一項具體實施例之無線LAN/MAN 70。在此項具體實施例中，工作站71、72已啟用如上文所述之有線等效保密(WEP)功能，因此會連同所傳送的所屬資料封包一起產生及傳輸完整性檢查值。因此，該監督站73偵測對該無線網路70之侵入的方法為，監視該等工作站71、72之間的傳輸，以便偵測不符合所屬資料封包的完整性檢查值。即，如果使用錯誤的金鑰流來產生訊息密文，或如果訊息已被惡意工作站84竄改過，則完整性檢查值很可能會出現訛誤。因此，當該監督站73偵測到此類錯誤的完整性檢查值時，就會據此產生一侵入警示，如熟悉此項技術者所知。

現在請參考圖8，現在說明根據本發明之另一種無線LAN/MAN 80。通常，當使用如上文所述的OSI網路模型時，則會產生各自的MAC序號，並且連同來自工作站81、82的每個資料封包一起傳送。也就是說，會隨著連續的資料封包來遞增MAC序號，因此每個封包都具有所相關的唯一

MAC序號。因此，該監督站83偵測對該無線網路80之侵入的方法為，監視該等工作站81、82之間的傳輸，以便偵測是否有一工作站使用非連續MAC序號，並且據此產生一侵入警示。

現在請參閱圖9，現在說明另一項替代具體實施例之無線LAN/MAN 90，其中該監督站93偵測對該無線網路之侵入的方法為，監視該等工作站91、92之間的傳輸，以便偵測是否有預先決定封包類型之封包衝突。具體而言，該預先決定封包類型可包含：管理訊框封包(例如，鑑認封包、關聯性封包及信標封包)、控制訊框封包(例如，RTS封包及CTS封包)及/或資料訊框封包。因此，該監督站93可依據偵測該預先決定封包類型的衝突臨限值次數來產生一侵入警示。

在本文中使用的用詞「衝突」預定包括同時傳輸封包，以及某時段內還有其他傳輸。即，如果假定某類型封包具有傳輸間時間延遲(例如，幾秒鐘)，如果兩種此類封包類型之傳輸極為接近(即，小於其之間的必要延遲時間)，則會視為衝突。舉例而言，衝突臨限值次數可大於(例如)約三，雖然也可使用其他臨限值。另外，臨限值次數可能係以考慮中的特定封包類型為基礎，即，臨限值次數因封包類型而異。

此外，臨限值次數可能係以所監視之具有預先決定封包類型之封包總數的百分比為基礎。例如，如果在一週期(例如，一小時)期間所傳輸之特定百分比(例如，大於約10%)

封包涉及衝突，則會產生侵入警示。或者，如果所監視之封包總數中的特定百分比封包(例如，總數10中有3個封包)涉及衝突，則會產生侵入警示。當然，還可使用其他適合的臨限值數量及建立臨限值數量的方法。

現在請參閱圖10，現在說明另一項替代具體實施例之無線LAN/MAN 100，其中該監督站103偵測對該無線網路之侵入的方法為，監視該等工作站101、102之間的傳輸，以便偵測是否有相同MAC位址之衝突。即，如果多個終端機處於同時要求同一MAC位址或彼此間極接近之狀態，則會發生錯誤或其中一個工作站是惡意工作站104。因此，該監督站103可依據偵測此類衝突臨限值次數(例如，大於約三)來產生一侵入警示。再次申明，也可使用其他臨限值，並且臨限值可能係以百分比為基礎，如上文所述。

現在將參考圖11來說明一種適用於無線網路10的本發明之侵入偵測方法觀點。從步驟110開始，該方法包括：在步驟111，複數個工作站11、12之間使用MAC層來傳輸資料，如上文所述。在步驟112，監視該等複數個工作站11、12之間的傳輸，以便偵測來自該等MAC位址之一的訊框檢查序列(FCS)錯誤。在步驟113，如果該MAC位址的FCS錯誤數量超過一臨限值，則在步驟114據此產生一侵入警示，因此而結束該方法(步驟115)。否則，會繼續監視傳輸作業，如圖所示。

現在參考圖12來說明本發明的第一項替代方法觀點。該方法從步驟120開始，在步驟121，複數個工作站21、22之

間正在傳輸資料，並且在步驟122監視傳輸作業，以便偵測鑑認MAC位址的失敗嘗試，如上文所述。在步驟123，如果偵測到數次鑑認一特定MAC位址的失敗嘗試，則在步驟124產生一侵入警示，因此而結束該方法(步驟125)。否則，會繼續監視侵入，如圖所示。

現在將參考圖13來說明本發明的第二項替代方法觀點。該方法從步驟130開始，在步驟131，複數個工作站31、32之間傳輸的RTS封包及CTS封包且接著傳輸資料。在步驟132，監視該等複數個工作站31、32之間傳送的該RTS封包及該CTS封包，以便偵測該等封包中的一非法NAV值，如上文所述。在步驟133，如果偵測到非法NAV值，則在步驟134據此產生一侵入警示，因此而結束該方法(步驟135)。否則，會繼續監視侵入，如圖所示。

現在請參考圖14，現在說明本發明的第三項替代方法觀點。該方法從步驟140開始，在步驟141，複數個工作站41、42之間正在傳輸資料，並且在步驟142監視傳輸作業，以便偵測非CFP期間的無競爭模式運作，如上文所述。在步驟143，如果在非CFP期間偵測到無競爭模式運作，則在步驟144據此產生一侵入警示，因此而結束該方法(步驟145)。否則，會繼續監視侵入，如圖所示。相反的案例如圖15之步驟150至步驟155所示，其中會監視傳輸以便偵測CFP期間的競爭模式運作。再次申明，可在單一具體實施例中運用這兩種方法，雖然這不是必要項。

現在將參考圖16來說明本發明的第四項方法觀點。該方

法從步驟160開始，在步驟161，複數個工作站61、62之間正在傳輸資料，並且在步驟162監視傳輸作業，以便偵測未經授權期間的傳輸，如上文所述。在步驟163，如果在未經授權期間偵測到傳輸，則在步驟164據此產生一侵入警示，因此而結束該方法(步驟165)。否則，會繼續監視侵入，如圖所示。

現在將參考圖17來說明本發明的另一項侵入偵測方法觀點。該方法從步驟170開始，在步驟171，複數個工作站71、72之間正在傳輸資料，並且在步驟172監視傳輸作業，以便偵測不符合所屬資料封包的完整性檢查值，如上文所述。在步驟173，如果偵測到不符合所屬資料封包的完整性檢查值，則在步驟174據此產生一侵入警示，因此而結束該方法(步驟175)。否則，會繼續監視侵入，如圖所示。

現在請參考圖18，說明本發明的另一項方法觀點。該方法從步驟180開始，在步驟181，複數個工作站81、82之間正在傳輸資料。因此，該方法也包括在步驟182監視傳輸以偵測是否有一工作站使用非連續MAC序號，如上文所述。在步驟183，如果偵測到工作站使用非連續MAC序號，則在步驟184產生一侵入警示，因此而結束該方法(步驟185)。否則，會繼續監視侵入，如圖所示。

現在請參考圖19，說明本發明的另一項方法觀點，該方法從步驟190開始，在步驟191，複數個工作站91、92之間正在傳輸資料，並且在步驟192，監視傳輸作業，以便偵測是否有預先決定封包類型之封包衝突，如上文所述。在步

驟193，如果偵測到該預先決定封包類型的衝突臨限值次數，則在步驟194產生一侵入警示，因此而結束該方法(步驟195)。否則，會繼續監視侵入，如圖所示。

現在將參考圖20來說明本發明的另一項侵入偵測方法觀點。該方法從步驟200開始，在步驟201，複數個工作站101、102之間正在傳輸資料，並且在步驟202監視傳輸作業，以便偵測是否有相同MAC位址之衝突，如上文所述。在步驟203，如果偵測到相同MAC位址的衝突臨限值次數，則在步驟204產生一侵入警示，因此而結束該方法(步驟205)。否則，會繼續監視侵入，如圖所示。

現在將參考圖21來說明本發明的進一步侵入偵測方法觀點。如上文所述，無線網路LAN/MAN通常具有相關的一或多個服務集ID，例如IBSSID、BSSID及/或ESSID。如圖所示，該方法從步驟210開始，在步驟211，複數個工作站11、12之間可傳輸資料，並且在步驟212，可監視複數個工作站之間的傳輸，以便偵測是否有非源自於經授權工作站之指定網路頻道相關的服務集ID及/或傳輸。

以此方式，如果在步驟213偵測到有一服務集ID不同於該無線網路10的一經授權服務集ID，及/或偵測到有來自未經授權之工作站的傳輸，則在步驟214據此產生一侵入警示。另外，在步驟215，可將該侵入警示傳輸至網路中的一或多個工作站(如上文所述)，或經由數據機將該侵入警示傳輸至其他來源。否則，會繼續監視侵入，如圖所示。

熟悉此項技術者應明白，在如上文所述之無線網路的一

施例的方塊圖，用於提供以非法網路配置向量(NAV)為基礎之侵入偵測。

圖4及圖5分別顯示圖1所示之無線LAN/MAN之進一步替代具體實施例的方塊圖，用於提供以非無競爭週期(CFP)期間之無競爭模式運作及CFP期間之競爭模式運作為基礎之侵入偵測。

圖6顯示圖1所示之無線LAN/MAN之另一項替代具體實施例的方塊圖，用於提供以未經授權週期期間發生之傳輸為基礎之侵入偵測。

圖7顯示圖1所示之無線LAN/MAN之另一項替代具體實施例的方塊圖，用於提供以偵測不符合所屬資料封包之完整性檢查值為基礎之侵入偵測。

圖8顯示圖1所示之無線LAN/MAN之另一項替代具體實施例的方塊圖，用於提供以偵測是否有一工作站使用非連續MAC序號為基礎之侵入偵測。

圖9顯示圖1所示之無線LAN/MAN之另一項替代具體實施例的方塊圖，用於提供以偵測是否具有預先決定封包類型之封包衝突為基礎之侵入偵測。

圖10顯示圖1所示之無線LAN/MAN之另一項替代具體實施例的方塊圖，用於提供以偵測相同MAC位址衝突為基礎之侵入偵測。

圖11顯示根據本發明之以偵測FCS錯誤為基礎之侵入偵測方法的流程圖。

圖12顯示根據本發明之以MAC位址鑑認失敗為基礎之侵

入偵測方法的流程圖。

圖13顯示根據本發明之以偵測非法網路配置向量(NAV)值為基礎之侵入偵測方法的流程圖。

圖14及圖15分別顯示根據本發明之以偵測非CFP期間之無競爭模式運作及偵測CFP期間之競爭模式運作為基礎之侵入偵測方法的流程圖。

圖16顯示根據本發明之以偵測未經授權週期期間發生之傳輸為基礎之侵入偵測方法的流程圖。

圖17顯示根據本發明之以偵測不符合所屬資料封包之完整性檢查值為基礎之侵入偵測方法的流程圖。

圖18顯示根據本發明之以偵測工作站是使用非連續MAC序號為基礎之侵入偵測方法的流程圖。

圖19顯示根據本發明之以偵測是否具有預先決定封包類型之封包衝突為基礎之侵入偵測方法的流程圖。

圖20顯示根據本發明之以偵測相同MAC位址衝突為基礎之侵入偵測方法的流程圖。

圖21顯示用以解說根據本發明之其他侵入偵測方法觀點的流程圖。

【圖式代表符號說明】

10，20，30，40，50，60，70，80，90，100	無線LAN/MAN(無線區域網路/無線大都會區域網路)
11，21，31，41，51，61，71，81，91，101	無線工作站

12，22，32，42，52，62，72，82，92，102	基地台(或存取點)
13，23，33，43，53，63，73，83，93，103	監督站
14，24，34，44，54，64，74，84，94，104	惡意工作站

伍、中文發明摘要：

本發明揭示一種無線區域網路或大都會區域網路，其可包括：複數個工作站，用於在該等工作站之間傳輸資料；以及一監督站。該監督站可藉由下列方式來偵測對該無線網路之侵入：監視該等複數個工作站之間的傳輸，以便偵測未經授權週期期間發生之傳輸；以及據此產生一侵入警示。該監督站也可以依據下列其中一或多項來偵測侵入：不符合所屬資料封包之完整性檢查值；工作站使用非連續媒體存取控制(MAC)序號；以及封包類型及/或MAC位址之衝突。

陸、英文發明摘要：

A wireless local or metropolitan area network may include a plurality of stations for transmitting data therebetween and a policing station. The policing station may detect intrusions into the wireless network by monitoring transmissions among the plurality of stations to detect transmissions during an unauthorized period and generate an intrusion alert based thereon. The policing station may also detect intrusions based upon one or more of integrity check values which do not correspond with respective data packets, usage of non-consecutive media access control (MAC) sequence numbers by a station, and collisions of packet types and/or MAC addresses.

拾、申請專利範圍：

1. 一種無線區域網路或大都會區域網路，包括：

複數個工作站，用於在該等工作站之間傳輸資料；以及

一監督站，用於偵測對該無線網路之侵入，偵測侵入的方式為監視該等複數個工作站之間的傳輸，以便偵測下列至少一項：

偵測是否有在未經授權期間進行傳輸；

在該等複數個工作站使用封包來傳輸資料並且產生要連同每個封包一起傳輸的所屬完整性檢查值的多個網路中，偵測是否有不符合所屬資料封包之完整性檢查值；

在該等複數個工作站經由一媒體存取控制(MAC)層來傳輸封包格式之資料並且還連同每個資料封包一起傳輸一所屬MAC序號的多個網路中，偵測是否有一工作站使用非連續MAC序號；

在該等複數個工作站使用具有相關封包類型之封包來傳輸資料的多個網路中，偵測具有預先決定封包類型之封包衝突是否達到一第一臨限值次數；

在該等複數個工作站經由一媒體存取控制(MAC)層傳輸資料並且每個工作站都具有一連同所傳送之資料一起傳輸的相關MAC位址之多個網路中，偵測一相同MAC位址的衝突是否達到一第二臨限值次數；

在該無線網路可具有相關的至少一服務集識別項

(ID)之多個網路中，偵測該等相關之服務集ID是否有不同於該無線網路的相關服務集ID；以及

在該等複數個工作站透過至少一頻道來傳輸資料的多個網路中，偵測是否有不是源自於該等複數個工作站之一的工作站透過該至少一頻道進行傳輸；以及接著

據此產生一侵入警示。

2. 如申請專利範圍第1項之無線網路，其中該預先決定封包類型可包含下列至少一項：鑑認封包、關聯性封包及信標封包、「要求傳送」(RTS)封包及「清除傳送」(CTS)。

3. 如申請專利範圍第1項之無線網路，其中該第一衝突臨限值次數及該第二衝突臨限值次數大於三。

4. 如申請專利範圍第1項之無線網路，其中該第一衝突臨限值次數係以所監視之具有預先決定封包類型之封包總數的百分比為基礎。

5. 如申請專利範圍第1項之無線網路，其中該監督站進一步將一侵入警示傳輸至該等複數個工作站中至少一工作站。

6. 一種運用在包含複數個工作站的無線區域網路或大都會區域網路之侵入偵測方法，該方法包括：

該等工作站之間正在傳輸資料，

監視該等複數個工作站之間的傳輸，以便偵測下列至少一項：

偵測是否有在未經授權期間進行傳輸；

在該等複數個工作站使用封包來傳輸資料並且產生要連同每個封包一起傳輸的所屬完整性檢查值的多個網路中，偵測是否有不符合所屬資料封包之完整性檢查值；

在該等複數個工作站經由一媒體存取控制(MAC)層來傳輸封包格式之資料並且還連同每個資料封包一起傳輸一所屬MAC序號的多個網路中，偵測是否有一工作站使用非連續MAC序號；

在該等複數個工作站使用具有相關封包類型之封包來傳輸資料的多個網路中，偵測具有預先決定封包類型之封包衝突；

在該等複數個工作站經由一媒體存取控制(MAC)層來傳輸資料的多個網路中，其中每個工作站都具有一要連同所傳送之資料一起傳輸的MAC位址，一相同MAC位址之衝突；

在該無線網路可具有相關的至少一服務集識別項(ID)之多個網路中，偵測該等相關之服務集ID是否有不同於該無線網路的相關服務集ID；以及

在該等複數個工作站透過至少一頻道來傳輸資料的多個網路中，偵測是否有不是源自於該等複數個工作站之一的工作站透過該至少一頻道進行傳輸；以及接著

據此產生一侵入警示。

柒、指定代表圖：

(一)本案指定代表圖為：第（ 6 ）圖。

(二)本代表圖之元件代表符號簡單說明：

60 無線LAN/MAN(無線區域網路/無線大都會區域網路)

61 無線工作站

62 基地台(或存取點)

63 監督站

64 惡意工作站

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

種或一種無線網路都可實施如上文所述之所有的方法觀點。再者，熟悉此項技術者可依據前面的說明內容瞭解到本發明的其他方法觀點，因此將不會在本文中詳細說明其他方法觀點。

顯而易見，可用各種方式來實施前文所說明的本發明。例如，可在不屬於無線網路10一部份的一或多個分離且專用的裝置中實施該監督站13。或者，本發明可實施為軟體，並且將實施本發明的軟體安裝在想要有侵入偵測功能之無線LAN/MAN中的一或多個現有工作站上。

另外，甚至當惡意工作站具有一經授權網路ID或MAC ID時，仍然可有利地運用許多如上文所述之本發明觀點來偵測網路侵入(例如，在非CFP期間偵測無競爭模式運作、在未經授權期間偵測傳輸等等)。另外，在既定應用中可有利地運用如上文所述之觀點中的一或多項觀點，以便提供所期望的侵入偵測等級。本發明的進一步優點為，可運用本發明來補充現有的侵入偵測系統，尤其是著重於較上層OSI網路層的侵入偵測系統。

【圖式簡單說明】

圖1顯示根據本發明之無線LAN/MAN的方塊圖，用於提供以訊框檢查序列(FCS)錯誤為基礎之侵入偵測。

圖2顯示圖1所示之無線LAN/MAN之替代具體實施例的方塊圖，用於提供以媒體存取控制(MAC)位址鑑認失敗為基礎之侵入偵測。

圖3顯示圖1所示之無線LAN/MAN之另一項替代具體實

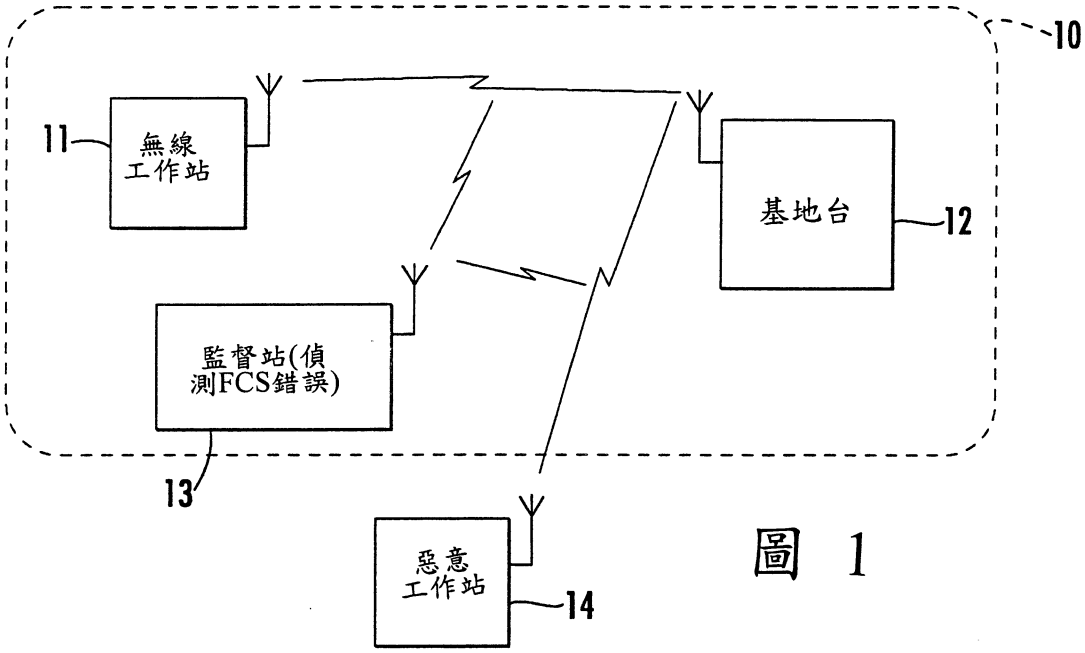
10
11
無線
工作站
基地台
12
監督站(偵
測FCS錯誤)
13
惡意
工作站
14

圖 1

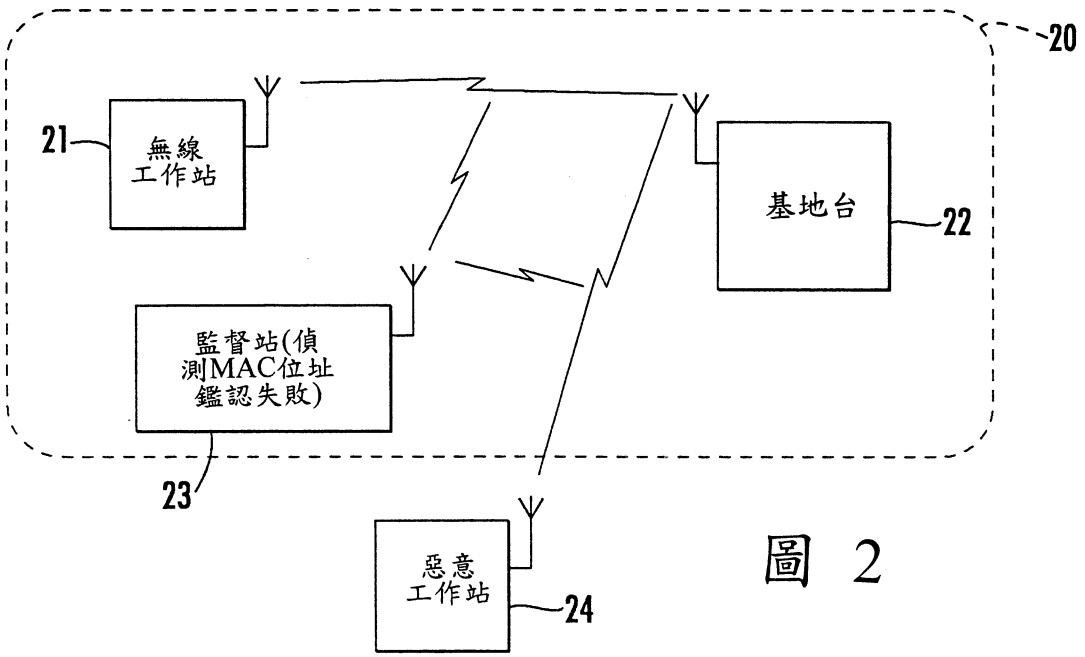
20
21
無線
工作站
基地台
22
監督站(偵
測MAC位址
鑑認失敗)
23
惡意
工作站
24

圖 2

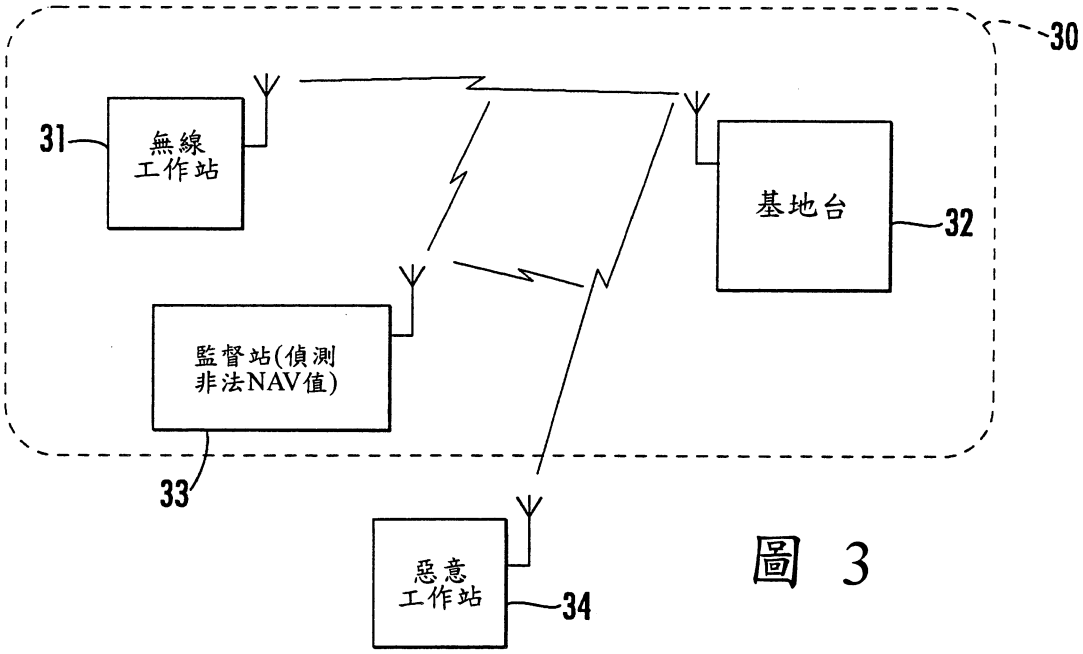
30
31
無線
工作站
基地台
32
監督站(偵測
非法NAV值)
33
惡意
工作站
34

圖 3

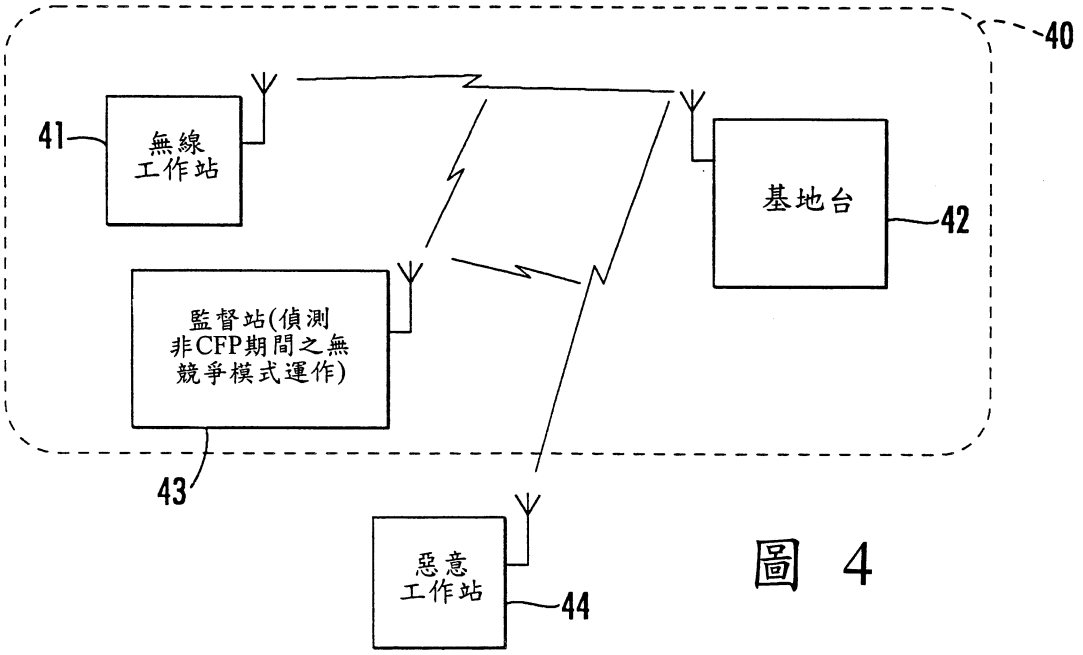
40
41
無線
工作站
基地台
42
監督站(偵測
非CFP期間之無
競爭模式運作)
43
惡意
工作站
44

圖 4

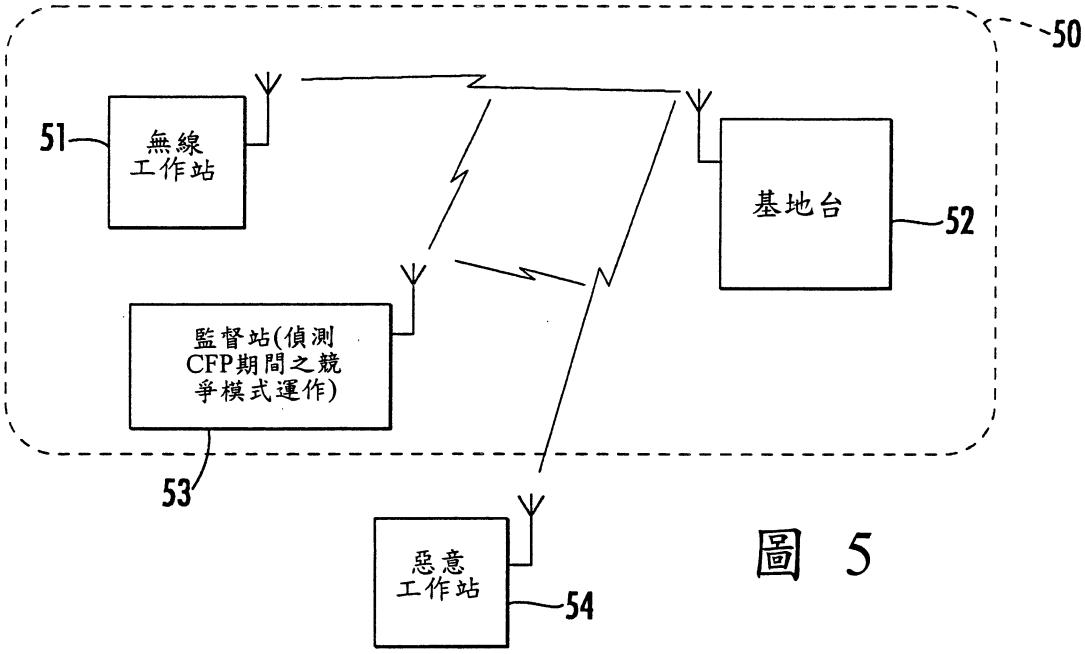
50
51
無線
工作站
基地台
52
監督站(偵測
CFP期間之競
爭模式運作)
53
惡意
工作站
54

圖 5

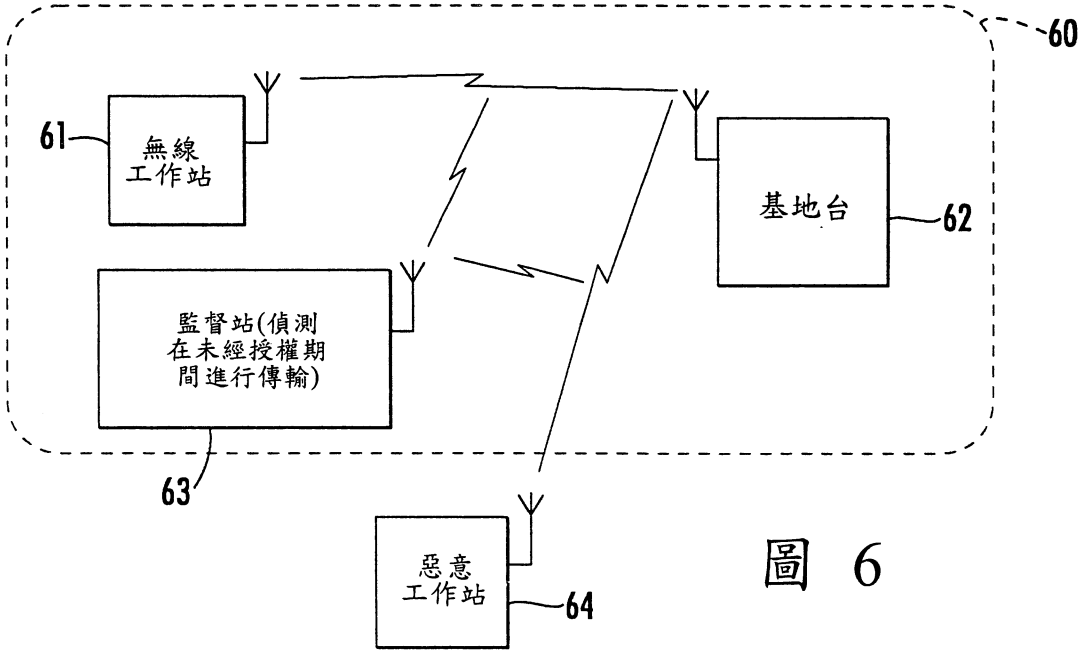
60
61
無線
工作站
基地台
62
監督站(偵測
在未經授權期
間進行傳輸)
63
惡意
工作站
64

圖 6

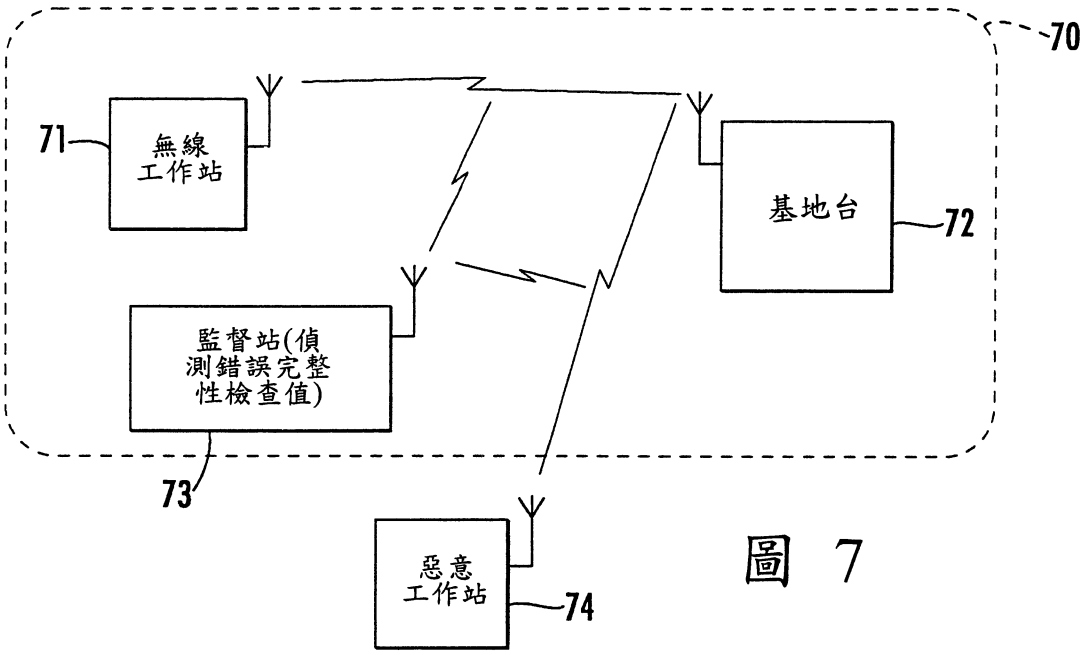
70
71
無線
工作站
基地台
72
監督站(偵
測錯誤完整
性檢查值)
73
惡意
工作站
74

圖 7

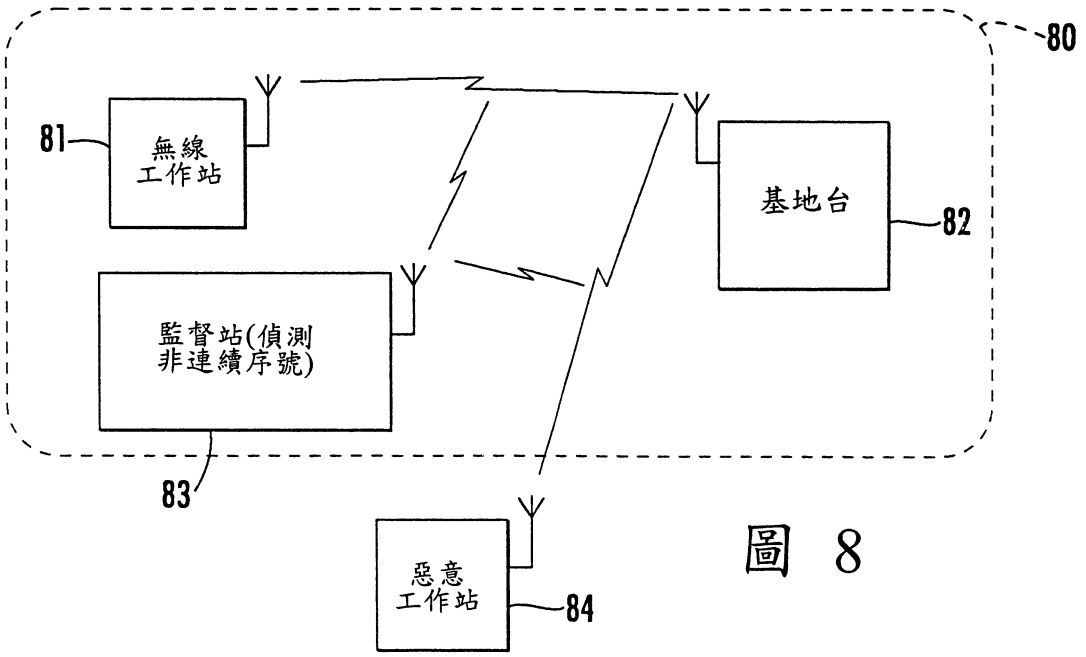
80
81
無線
工作站
基地台
82
監督站(偵測
非連續序號)
83
惡意
工作站
84

圖 8

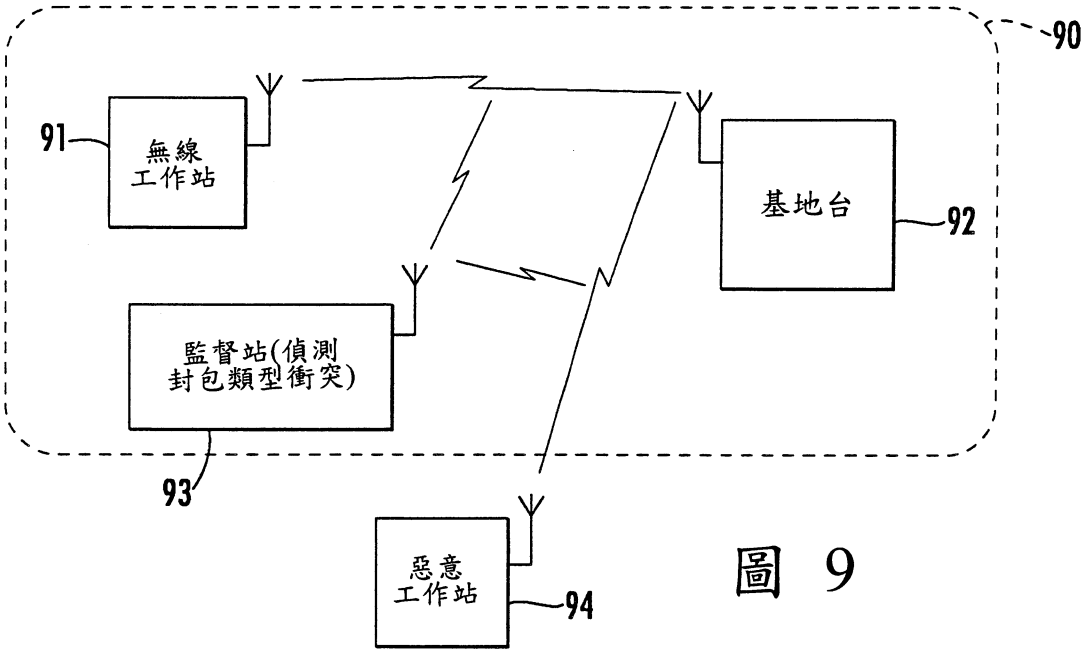
90
91
無線
工作站
基地台
92
監督站(偵測
封包類型衝突)
93
惡意
工作站
94

圖 9

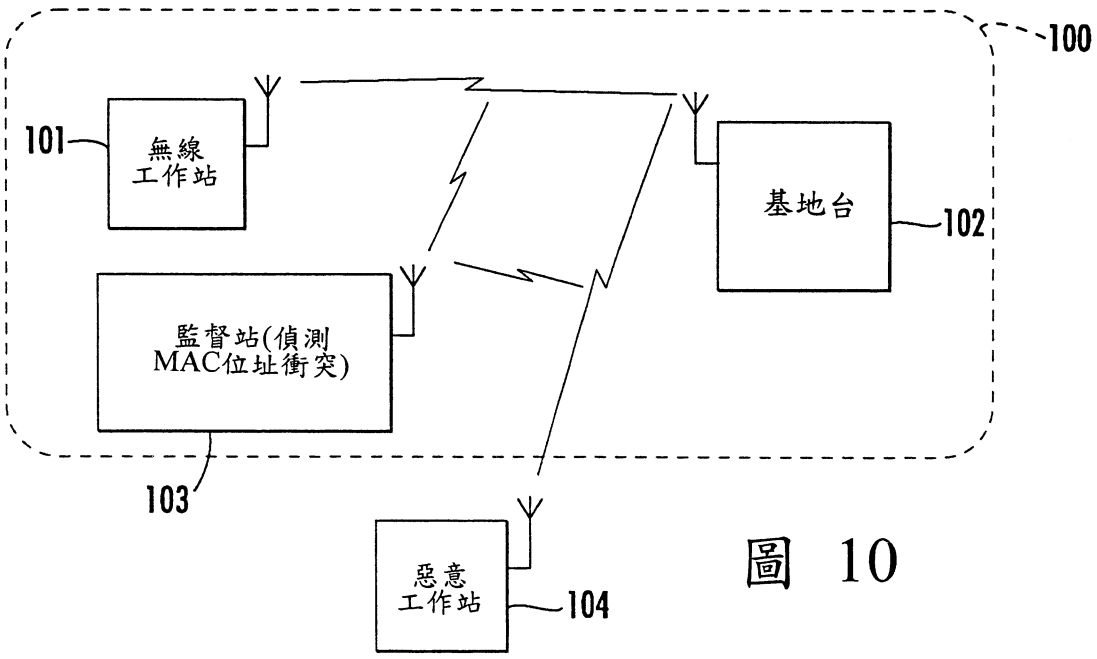
100
101
無線
工作站
基地台
102
監督站(偵測
MAC位址衝突)
103
惡意
工作站
104

圖 10

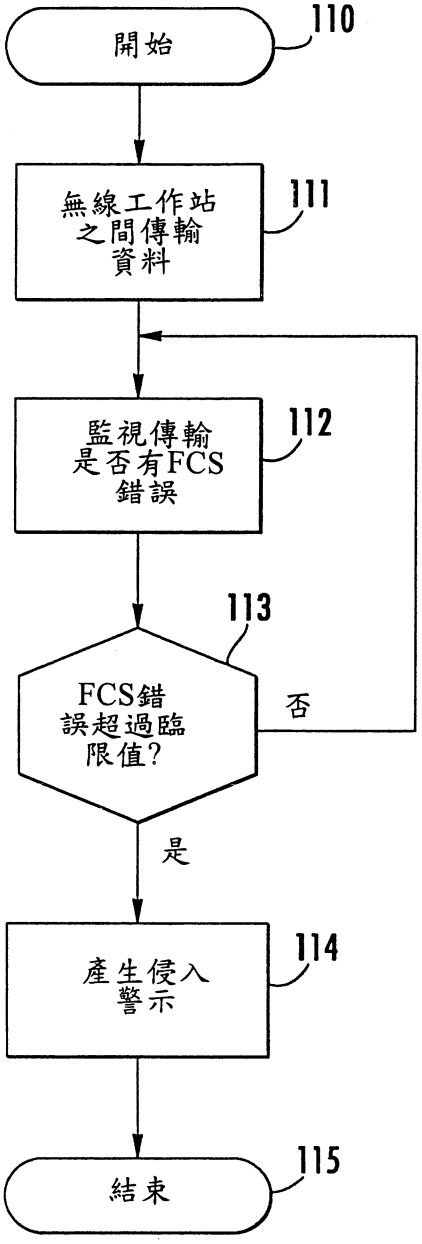
開始
110
無線工作站之間傳輸資料
111
監視傳輸是否有FCS錯誤
112
FCS錯誤超過臨限值?
113
否
是
產生侵入警示
114
結束
115

圖 11

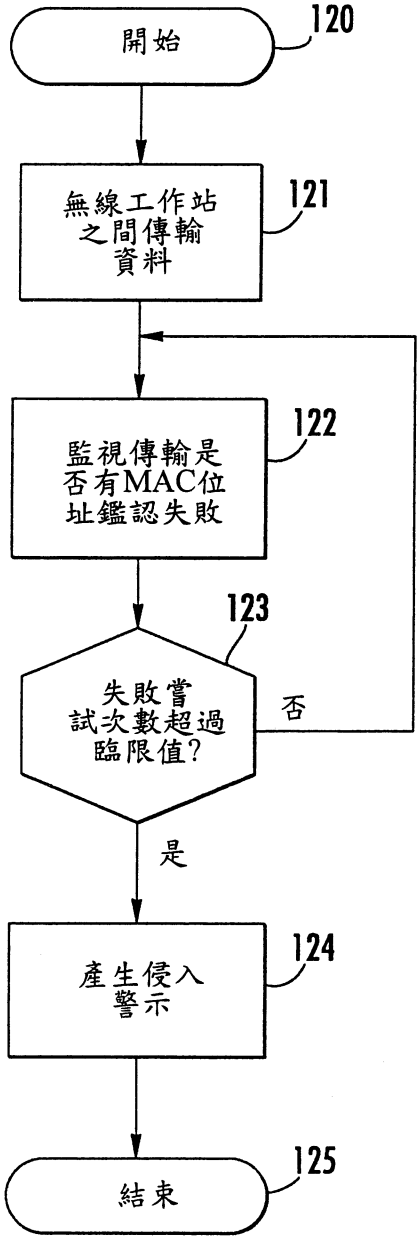
開始
120
無線工作站之間傳輸資料
121
監視傳輸是否有MAC位址鑑認失敗
122
失敗嘗試次數超過臨限值?
123
否
是
產生侵入警示
124
結束
125

圖 12

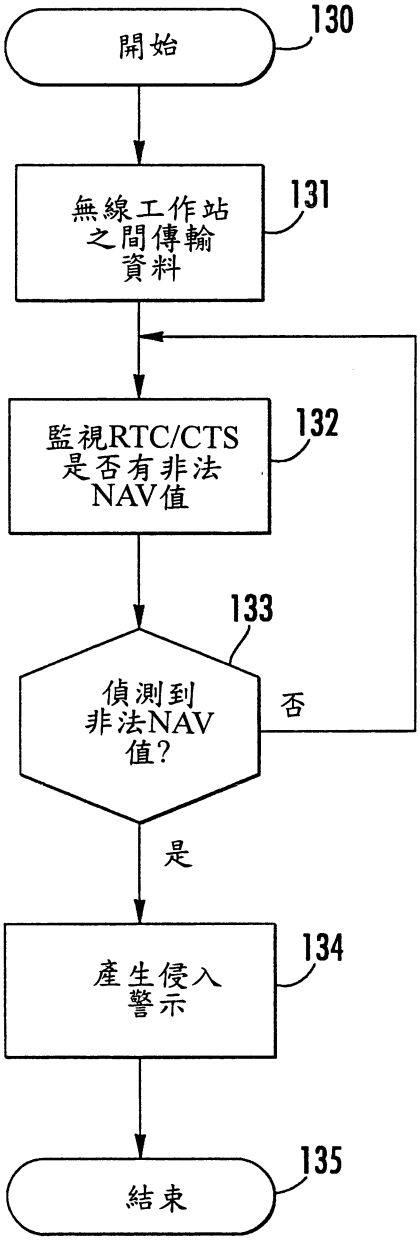
開始
130
無線工作站之間傳輸資料
131
監視RTC/CTS是否有非法NAV值
132
偵測到非法NAV值?
133
否
是
產生侵入警示
134
結束
135

圖 13

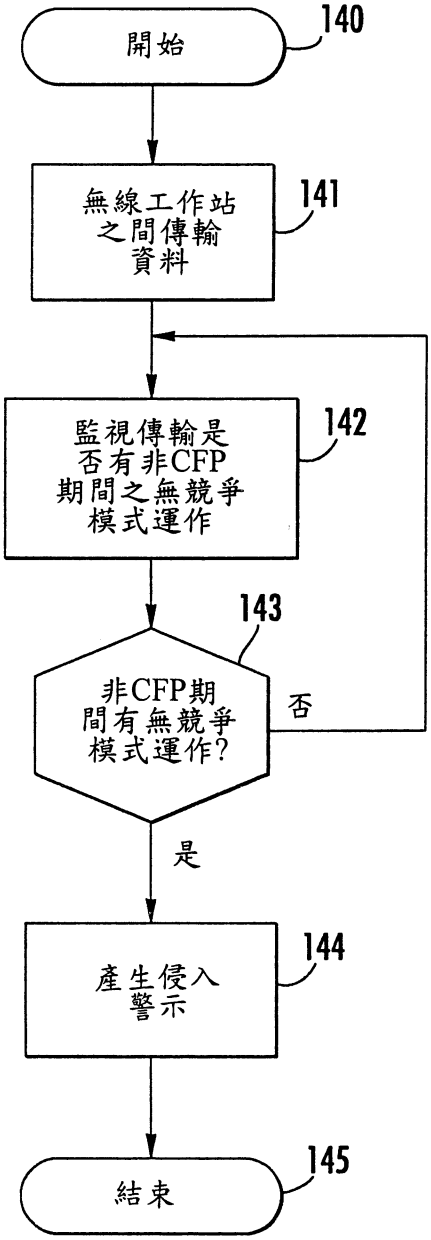
開始
140
無線工作站之間傳輸資料
141
監視傳輸是否有非CFP期間之無競爭模式運作
142
非CFP期間有無競爭模式運作?
143
否
是
產生侵入警示
144
結束
145

圖 14

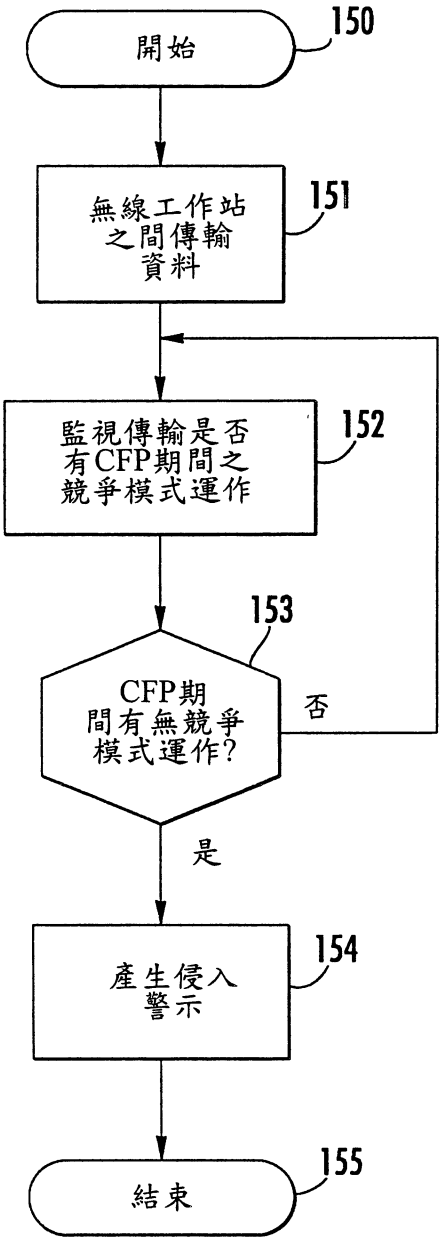
開始
150
無線工作站之間傳輸資料
151
監視傳輸是否有CFP期間之競爭模式運作
152
CFP期間有無競爭模式運作?
153
否
是
產生侵入警示
154
結束
155

圖 15

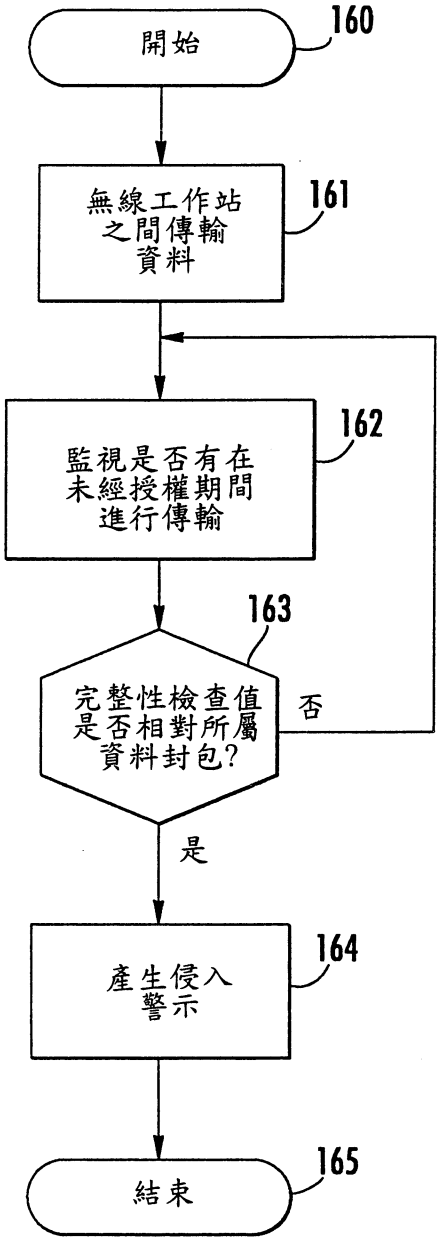
開始
160
無線工作站之間傳輸資料
161
監視是否有在未經授權期間進行傳輸
162
完整性檢查值是否相對所屬資料封包?
163
否
是
產生侵入警示
164
結束
165

圖 16

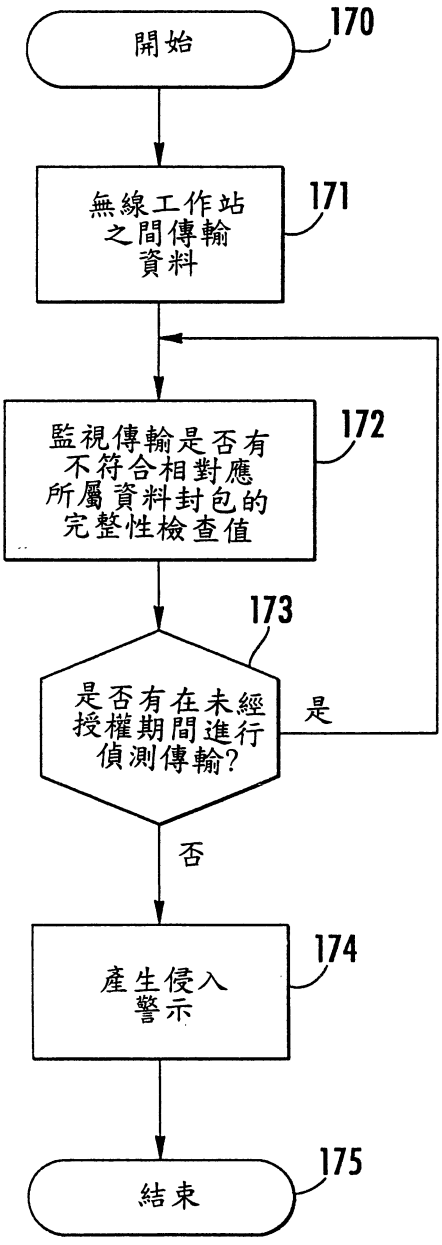
開始
170
無線工作站之間傳輸資料
171
監視傳輸是否有不符合相對應所屬資料封包的完整性檢查值
172
173
是否有在未經授權期間進行偵測傳輸?
是
否
產生侵入警示
174
結束
175

圖 17

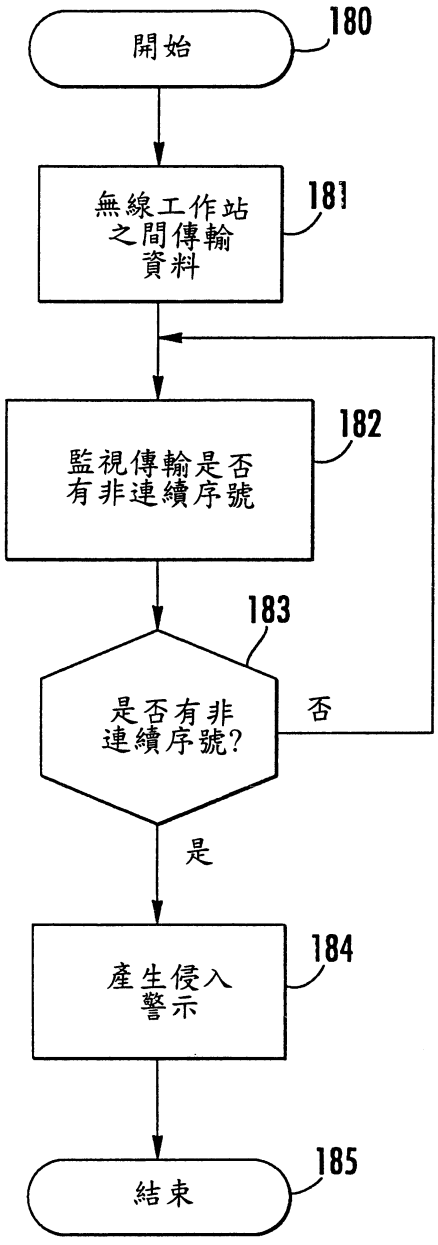
開始
180
無線工作站之間傳輸資料
181
監視傳輸是否有非連續序號
182
183
是否有非連續序號?
否
是
產生侵入警示
184
結束
185

圖 18

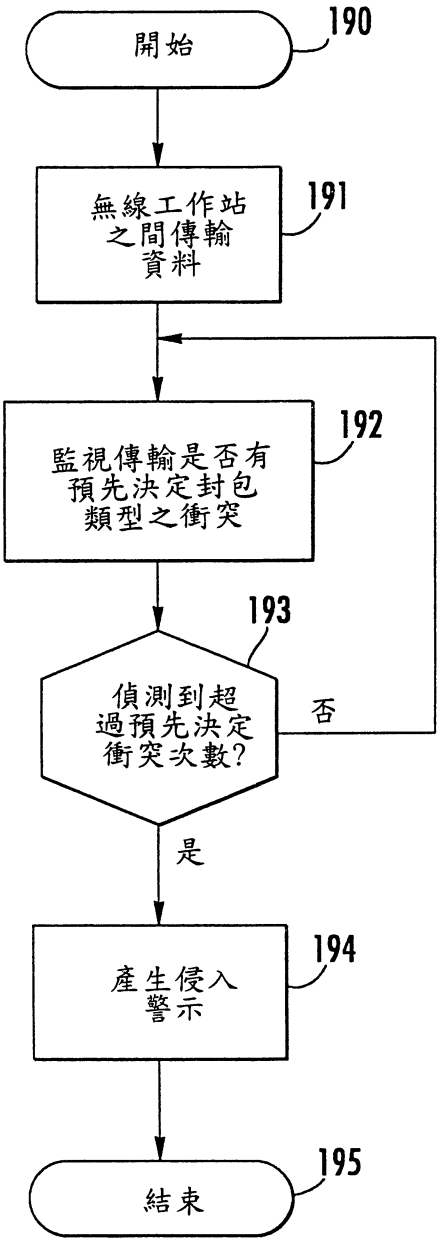
開始
190
無線工作站之間傳輸資料
191
監視傳輸是否有預先決定封包類型之衝突
192
偵測到超過預先決定衝突次數?
193
否
是
產生侵入警示
194
結束
195

圖 19

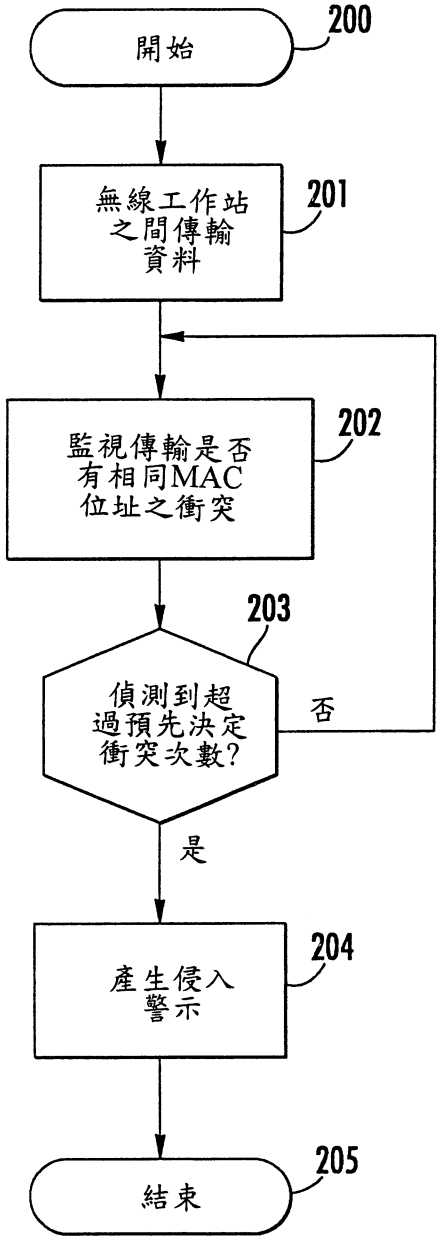
開始
200
無線工作站之間傳輸資料
201
監視傳輸是否有相同MAC位址之衝突
202
偵測到超過預先決定衝突次數?
203
否
是
產生侵入警示
204
結束
205

圖 20

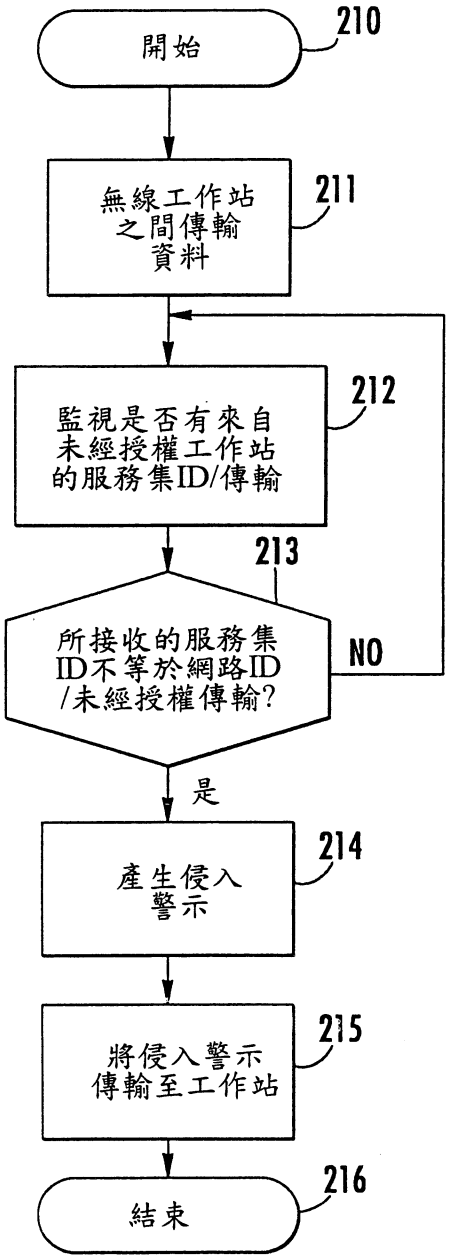
開始
210
無線工作站之間傳輸資料
211
監視是否有來自未經授權工作站的服務集ID/傳輸
212
213
所接收的服務集ID不等於網路ID/未經授權傳輸?
NO
是
產生侵入警示
214
將侵入警示傳輸至工作站
215
結束
216

圖 21