I721693

(19)中華民國智慧財產局

(12)發明說明書公告本　**(11)證書號數：TW I721693 B**

(45)公告日： 中華民國 110 (2021) 年 03 月 11 日

(21)申請案號：108144919　(22)申請日： 中華民國 108 (2019) 年 12 月 09 日

(51)Int. Cl.：　*H04L12/26　(2006.01)*　*H04L29/06　(2006.01)*

G06F11/34　(2006.01)

(71)申請人：中華電信股份有限公司 (中華民國) CHUNGHWA TELECOM CO., LTD.　(TW)

桃園市楊梅區電研路 99 號

(72)發明人：王柏崴 WANG, PO WEI (TW) ；陳俊廷 CHEN, JIUN TING (TW) ；梁原誠 LIANG, YUAN CHENG (TW)

(74)代理人：林長榮

(56)參考文獻：

JP　2018513457A

審查人員：林宥辰

申請專利範圍項數：14 項　　圖式數：8　　共 30 頁

(54)名稱

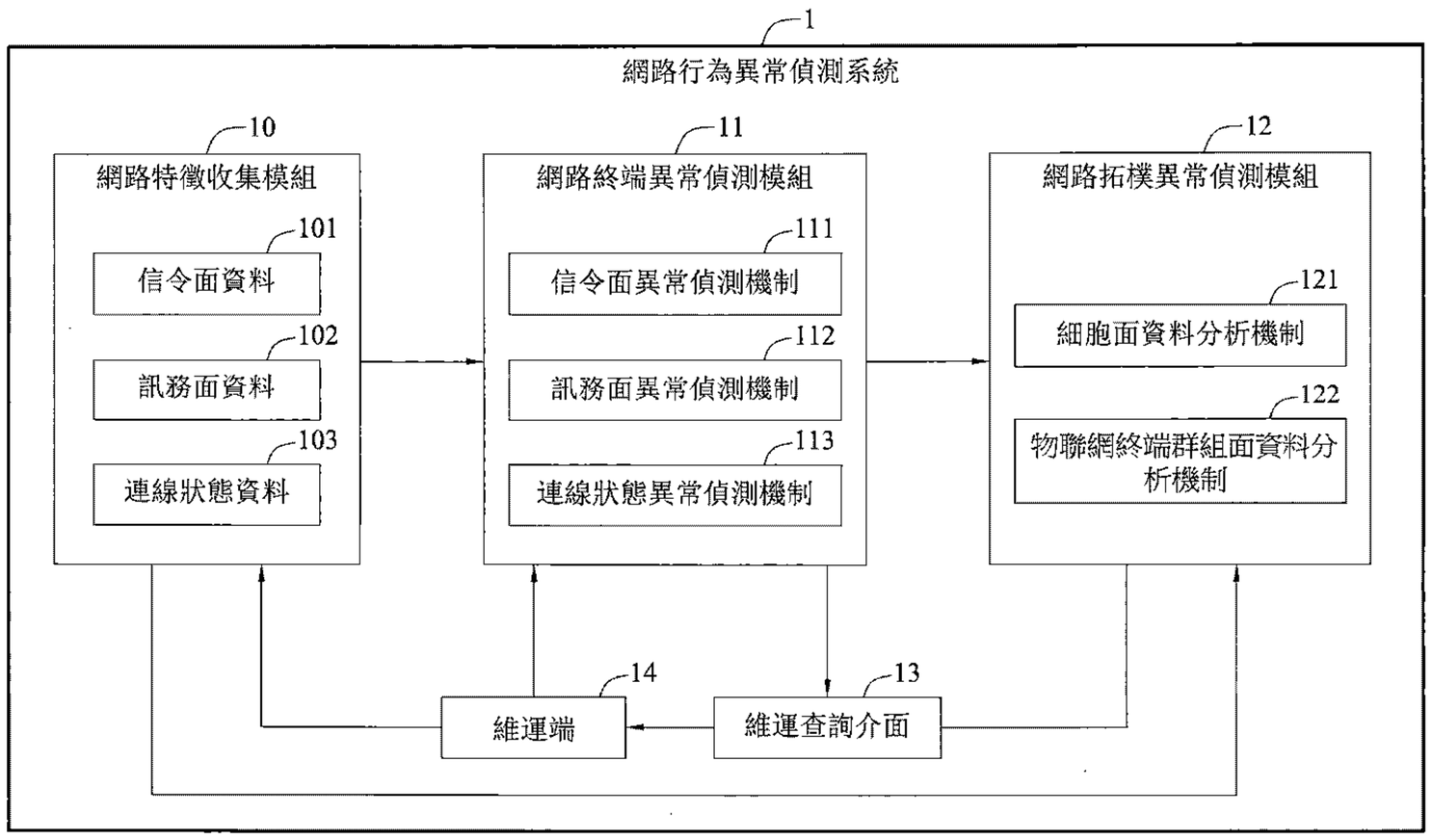
基於行動物聯網之網路行為異常偵測系統及方法

(57)摘要

本發明提供一種基於行動物聯網之網路行為異常偵測系統及方法。此系統包括網路終端異常偵測模組與網路拓樸異常偵測模組。網路終端異常偵測模組係具有信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制，以分別偵測網路終端之信令面、訊務面與連線狀態三者之異常。網路拓樸異常偵測模組係具有細胞面資料分析機制與物聯網終端群組面資料分析機制，以分別偵測細胞與物聯網終端群組二者之異常。

The invention discloses network behavior anomaly detection system and method based on mobile internet of things (IoT). The system includes a network terminal anomaly detection module and a network topology anomaly detection module. The network terminal anomaly detection module has a signaling anomaly detection mechanism, a traffic anomaly detection mechanism and a connection state anomaly detection mechanism to respectively detect abnormalities of the signaling, the traffic and the connection state of the network terminal. The network topology anomaly detection module has a cell data analysis mechanism and an IoT terminal group data analysis mechanism to detect abnormalities of the cell and the IoT terminal group.

指定代表圖：



【第1圖】

符號簡單說明：

1・・・網路行為異常偵測系統

10・・・網路特徵收集模組

101・・・信令面資料

102・・・訊務面資料

103・・・連線狀態資料

11・・・網路終端異常偵測模組

111・・・信令面異常偵測機制

112・・・訊務面異常偵測機制

113・・・連線狀態異常偵測機制

12・・・網路拓樸異常偵測模組

121・・・細胞面資料分析機制

122・・・物聯網終端群組面資料分析機制

13・・・維運查詢介面

14・・・維運端

公告本

【發明摘要】

【中文發明名稱】 基於行動物聯網之網路行為異常偵測系統及方法

【英文發明名稱】 NETWORK BEHAVIOR ANOMALY DETECTION SYSTEM AND METHOD BASED ON MOBILE INTERNET OF THINGS

【中文】

本發明提供一種基於行動物聯網之網路行為異常偵測系統及方法。此系統包括網路終端異常偵測模組與網路拓樸異常偵測模組。網路終端異常偵測模組係具有信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制，以分別偵測網路終端之信令面、訊務面與連線狀態三者之異常。網路拓樸異常偵測模組係具有細胞面資料分析機制與物聯網終端群組面資料分析機制，以分別偵測細胞與物聯網終端群組二者之異常。

【英文】

The invention discloses network behavior anomaly detection system and method based on mobile internet of things (IoT). The system includes a network terminal anomaly detection module and a network topology anomaly detection module. The network terminal anomaly detection module has a signaling anomaly detection mechanism, a traffic anomaly detection mechanism and a connection state anomaly detection mechanism to respectively detect abnormalities of the signaling, the traffic and the

connection state of the network terminal. The network topology anomaly detection module has a cell data analysis mechanism and an IoT terminal group data analysis mechanism to detect abnormalities of the cell and the IoT terminal group.

【指定代表圖】　　第1圖

【代表圖之符號簡單說明】

1	網路行為異常偵測系統	10	網路特徵收集模組
101	信令面資料	102	訊務面資料
103	連線狀態資料	11	網路終端異常偵測模組
111	信令面異常偵測機制	112	訊務面異常偵測機制
113	連線狀態異常偵測機制	12	網路拓樸異常偵測模組
121	細胞面資料分析機制	122	物聯網終端群組面資料分析機制
13	維運查詢介面	14	維運端

【特徵化學式】

本案無化學式。

【發明說明書】

【中文發明名稱】 基於行動物聯網之網路行為異常偵測系統及方法

【英文發明名稱】 NETWORK BEHAVIOR ANOMALY DETECTION SYSTEM AND METHOD BASED ON MOBILE INTERNET OF THINGS

【技術領域】

【0001】本發明是關於一種網路行為異常偵測技術，詳而言之，是有關於一種基於行動物聯網之網路行為異常偵測系統及方法。

【先前技術】

【0002】近年來，隨著行動物聯網之業務的持續成長，物聯網終端數大量增加，使得各家行動網路業者皆積極佈建物聯網監測系統，以求能迅速掌握物聯網終端的連線狀況並優化自家網路品質。

【0003】習知物聯網之網路行為異常偵測技術需在物聯網終端上進行分析，或是在部分終端加上額外裝置。然而，此習知技術除了取樣數量有限外，也會導致成本的急劇增加。特別是，由於物聯網終端的數量龐大且散佈在各地，因此透過人力進行監測與維運之效率明顯欠佳，也難以掌握各個終端的確實狀態。又，因為難以判定終端是否真的發生異常，所以無法對異常終端的網路行為進行貼標。再者，由於缺乏判斷物聯網終端異常之自動化機制，加上偵測方式不夠全面，精準率不高，導致行動業者難以掌握大量物聯網終端的運作狀況。

【0004】因此，如何提供一種新穎或創新之基於行動物聯網之網路行為異常偵測技術，實已成為本領域技術人員之一大研究課題。

【發明內容】

【0005】本發明提供一種基於行動物聯網之網路行為異常偵測系統，包括：網路終端異常偵測模組，係具有信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制，以分別偵測網路終端之信令面、訊務面與連線狀態三者之異常；以及網路拓樸異常偵測模組，係具有細胞面資料分析機制與物聯網終端群組面資料分析機制，以分別偵測細胞與物聯網終端群組二者之異常。

【0006】在一實施例中，網路行為異常偵測系統係包括一網路特徵收集模組，用以收集行動網路之信令面資料、訊務面資料與連線狀態資料，並對信令面資料、訊務面資料與連線狀態資料進行彙整與預處理。

【0007】在一實施例中，網路特徵收集模組係執行下列程序：判斷是否有網路終端之歷史資料，若無歷史資料，則進行歷史分時資料收集，以取得預定期間內行動網路之信令面資料、訊務面資料與網路終端之離線時間；收集最新分時資料，以取得行動網路之信令面資料與訊務面資料；以及對歷史分時資料與最新分時資料進行彙整與預處理，且更新歷史資料。

【0008】在一實施例中，網路終端異常偵測模組之信令面異常偵測機制係包括下列程序：定期匯入網路終端的信令面歷史資料，根據信令面歷史資料重新訓練信令面異常判定模型以更新模型參數；匯入網路終端的信令面最新分時資料；使用信令面異常判定模型進行異常判定；以及匯出異常網路終端清單。

【0009】在一實施例中，信令面異常判定模型係用以進行異常樣本認定與異常肇因推測，其中，異常樣本認定是透過離群值判定演算法來認定，而異常肇因推測是彙整與記錄導致離群的行為特徵。

【0010】在一實施例中，網路終端異常偵測模組之訊務面異常偵測機制係包括下列程序：定期匯入網路終端的訊務面歷史資料；根據訊務面歷史資料重新訓練訊務面異常判定模型；使用訊務面異常判定模型預測網路終端當日的運作軌跡；匯入網路終端的訊務面最新分時資料；偵測網路終端是否異常；以及匯出異常網路終端清單。

【0011】在一實施例中，訊務面異常判定模型為一時間序列模型，例如整合移動平均自迴歸(Autoregressive Integrated Moving Average; ARIMA)模型，所述預測網路終端當日的運作軌跡包括預測值與信賴區間，且所述偵測網路終端是否異常係透過比較預測值與實際值而判定。

【0012】在一實施例中，網路終端異常偵測模組之連線狀態異常偵測機制係包括下列程序：匯入各物聯網終端群組的離線時間歷史資料；使用一離線時間門檻值認定模型決定各物聯網終端群組的離線門檻；即時判定各物聯網終端群組中網路終端的連線狀態，若判定連線狀態為離線，則根據離線門檻判定網路終端的離線期間是否過長；以及匯出有離線期間過長之網路終端及其離線時間。

【0013】在一實施例中，離線時間門檻值認定模型係透過單變量分群演算法來決定離線門檻。

【0014】在一實施例中，網路拓樸異常偵測模組之細胞面資料分析機制係包括下列程序：進行駐留細胞判定，其中，透過選取網路終端連線最頻繁之細胞，且細胞在最近一段期間內所連線之網路終端數目超過一預定門檻而認定細胞為駐留細胞；匯入行動網路之信令面資料、訊務面資料及各網路終端之連線狀態資料，並篩選與駐留細胞相關的資料；以及分別由信令面、訊務面與連線狀態來判定各駐留細胞是否異常。

【0015】在一實施例中，網路拓樸異常偵測模組之物聯網終端群組面

資料分析機制係包括下列程序：將各物聯網終端群組中最近一段期間內曾上線之網路終端設定為活躍網路終端；匯入行動網路之信令面資料、訊務面資料及各網路終端之連線狀態資料，並篩選與活躍網路終端相關的資料；以及分別由信令面、訊務面與連線狀態來判斷各物聯網終端群組是否異常。

【0016】本發明亦提供一種行基於動物聯網之網路行為異常偵測方法，包括：擷取行動網路之信令面資料、訊務面資料與連線狀態資料；使用離群值演算法處理信令面資料，以偵測行動網路之信令面是否異常；使用時間序列模型處理訊務面資料並進行預測，以判定行動網路之訊務面是否異常；以及使用單變量分群演算法處理連線狀態資料，以偵測行動網路連線狀態是否異常。

【0017】在一實施例中，網路行為異常偵測方法更包括：進行駐留細胞判定；篩選屬於駐留細胞的信令面資料、訊務面資料與連線狀態資料；以及分別由信令面、訊務面與連線狀態來判定駐留細胞是否異常。

【0018】在一實施例中，網路行為異常偵測方法更包括：從各物聯網終端群組中找出近期曾連線之網路終端；篩選與網路終端相關的信令面資料、訊務面資料與連線狀態資料；以及分別由信令面、訊務面與連線狀態來判斷各物聯網終端群組是否異常。

【0019】本發明之基於行動物聯網之網路行為異常偵測系統及方法係至少具有下列優點或技術功效。

【0020】首先，透過收集行動網路資料，將終端與局端之間的連線行為，以時間序列、離群值等人工智慧演算法建構出物聯網終端異常行為偵測模型，因此能有效的分析行動物聯網之全體終端的實際使用狀況，且可以無須如習知技術般在各終端進行觀測。又，即使當任意的物聯網終端損壞而斷線失聯，亦能透過本發明之偵測模型在第一時間偵測發現異常，不

影響運作性能。

【0021】再者，本發明的信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制，可分別針對信令、流量與連線狀態進行全面的異常行為偵測，且相關的偵測機制全程自動化，因此能有效提升維運大量物聯網終端的效率。

【0022】另外，由於本發明的訓練模型導入了移動窗格的概念，可定期(例如每日或每小時)依照最新收集到的資料來調整偵測模型，因此能充分且有效的因應物聯網終端行為的變化趨勢。

【圖式簡單說明】

【0023】第 1 圖顯示本發明之基於行動物聯網之網路行為異常偵測系統的示意方塊圖；

【0024】第 2 圖顯示本發明之網路特徵收集模組的運作流程圖；

【0025】第 3 圖顯示本發明之信令面異常偵測機制的流程圖；

【0026】第 4 圖顯示本發明之訊務面異常偵測機制的流程圖；

【0027】第 5 圖顯示本發明之連線狀態異常偵測機制的流程圖；

【0028】第 6 圖顯示本發明之細胞面資料分析機制的流程圖；

【0029】第 7 圖顯示本發明之物聯網終端群組面資料分析機制的流程圖；以及

【0030】第 8 圖顯示本發明之基於行動物聯網之網路行為異常偵測方法的流程圖。

【實施方式】

【0031】以下藉由特定的具體實施例說明本發明之實施方式，熟悉此

技藝之人士可由本說明書所揭示之內容輕易地瞭解本發明之優點及功效。

【0032】第 1 圖顯示本發明之基於行動物聯網之網路行為異常偵測系統 1 的示意方塊圖，此網路行為異常偵測系統 1 的主要元件包括一網路終端異常偵測模組 11 與一網路拓樸異常偵測模組 12，例如網路終端異常偵測模組 11 或網路拓樸異常偵測模組 12 可為硬體之偵測器或軟體之偵測程式等。網路終端異常偵測模組 11 包括一信令面異常偵測機制 111、一訊務面異常偵測機制 112 與一連線狀態異常偵測機制 113，以分別偵測網路終端之信令面、訊務面與連線狀態三者之異常。網路拓樸異常偵測模組 12 包括一細胞面資料分析機制 121 與一物聯網終端群組面資料分析機制 122，以分別偵測細胞與物聯網終端群組二者之異常。此處所稱細胞係指行動網路之基地台。

【0033】如第 1 圖所示，網路行為異常偵測系統 1 可包括一網路特徵收集模組 10，例如硬體之收集器或軟體之收集程式等。網路特徵收集模組 10 可以收集網路終端之信令面資料 101、訊務面資料 102 與連線狀態資料 103，並對信令面資料 101、訊務面資料 102 與連線狀態資料 103 進行彙整與預處理。網路特徵收集模組 10 所收集彙整之行動網路資料可提供給網路終端異常偵測模組 11 與網路拓樸異常偵測模組 12，以供網路終端異常偵測模組 11 與網路拓樸異常偵測模組 12 根據這些行動網路資料進行異常偵測及判定。

【0034】在一實施例中，網路特徵收集模組 10 可利用一訊號擷取單元，以自動且定時擷取網路終端在網路上跨介面的信令與訊務資料，並從信令面進行網路終端的上網連線行為及離線資訊分析，且從訊務面進行網路終端的應用服務的上網資訊分析。因此，網路特徵收集模組 10 能定期彙整特定物聯網之網路終端的資料，並同時進行資料預處理，再將預處理的

結果儲存於一資料庫中，以提供後續網路終端異常偵測模組 11 與網路拓樸異常偵測模組 12 所需之模型訓練及自動化偵測機制來使用。

【0035】根據網路特徵收集模組 10 所生成各面向資料，網路終端異常偵測模組 11 可執行信令面異常偵測機制 111、訊務面異常偵測機制 112 與連線狀態異常偵測機制 113，透過離群值演算法與時間序列分析等方法對網路終端進行各面向的異常偵測，並將異常偵測的結果儲存於資料庫中，以供維運查詢介面 13 及網路拓樸異常偵測模組 12 後續分析來使用。同時，網路終端異常偵測模組 11 亦會根據維運端 14 於偵測驗證結果及回饋來修正演算法與模型參數。此外，維運人員也可經由維運端 14 提供欲收集網路終端的門號清單給網路特徵收集模組 10。

【0036】所述網路拓樸異常偵測模組 12 負責針對各種網路拓樸的偵測基準進行分析。可套用的網路拓樸，除了上述提到的細胞與物聯網終端群組外，尚可套用至存取點名稱(Access Point Name; APN)等，或延伸至各種行動網路元件(如封包閘道器(Packet Gateway))等。在本實施例中，以細胞及物聯網終端群組為例，網路拓樸異常偵測模組 12 可包括細胞面資料分析機制 121 與物聯網終端群組面資料分析機制 122，利用網路特徵收集模組 10 與網路終端異常偵測模組 11 所產出之統計資料及異常清單對資料進一步整合，並利用所設定的網路拓樸分析邏輯來偵測異常狀態，可將結果寫入資料庫或任何儲存媒介以供維運人員存取使用。

【0037】值得注意的是，所述網路特徵收集模組 10、網路終端異常偵測模組 11 與網路拓樸異常偵測模組 12 等多個模組可部署於同一硬體平台，且多個模組之間的通訊藉由程式介面來進行；或者，也可部署於不同硬體平台，多個模組之間的通訊藉由 IP(Internet Protocol; 網際網路協定)基礎之通訊協定來進行。例如，本發明可實施之行動網路包括 UMTS(通用移動通

訊系統)行動網路、LTE(長期演進技術)行動網路、5G 行動網路等，但不以此為限。

【0038】第 2 圖顯示本發明之網路特徵收集模組 10 的運作流程圖並包括下列步驟，且參照第 1 圖予以說明。首先，網路特徵收集模組 10 可定期(例如每日)判斷是否有網路終端之歷史資料(步驟 S21)。亦即，判斷維運人員列於門號清單中關注的網路終端是否有歷史資料可提供模型訓練。若無歷史資料，則重新收集歷史分時資料(步驟 S22)，以取得預定期間內行動網路之信令面資料 101、訊務面資料 102 與網路終端之離線時間。若有歷史資料，則可直接讀取歷史資料(步驟 S23)。另一方面，定期(例如每小時)收集最新分時資料(步驟 S24)，以取得行動網路最新的信令面資料 101 與訊務面資料 102。隨後，對所取得的歷史分時資料與最新分時資料進行資料彙整與預處理(步驟 S25)，再更新歷史資料且匯出最新資料(步驟 S26)。

【0039】在一實施例中，若以 LTE 行動網路為例，上述信令面資料 101 可包括各網路終端於每小時之控制信令數(例如，Attach、Track Area Update、Handover、Path Switch、Service Request (正常)、Service Request (異常)、Control Plane Service Request、ESM data transport)、駐留細胞數，且訊務面資料 102 可包括網路終端的下載傳輸量、上載傳輸量、下行吞吐量、上行吞吐量、LTE 封包數比率等資訊。此外，也可從行動網路之計費信令(如 Radius accounting)資料中彙整網路終端的離線資訊。

【0040】第 3 圖顯示本發明之信令面異常偵測機制的流程圖並包括下列步驟。首先，可定期(例如每日)匯入網路終端的信令面歷史資料(步驟 S31)。接著，根據信令面歷史資料訓練信令面異常判定模型(步驟 S32)，以更新模型參數。另一方面，可匯入網路終端的信令面最新分時資料(步驟 S33)，並使用更新後的信令面異常判定模型進行異常判定(步驟 S34)。在完成異常判

定後，可匯出異常網路終端清單(步驟 S35)。

【0041】所述信令面異常判定模型主要用以進行異常樣本認定與異常肇因推測，其中異常樣本認定是透過離群值判定演算法(例如，孤立森林(Isolation Forest)及/或局部異常因子(Local Outlier Factor))來進行，目的是為了辨別行為特殊之離群值樣本，並將離群值樣本視為異常。在設定離群值比率與訓練資料後，可判定同樣分佈資料是否為離群。同時，異常肇因推測是彙整與記錄導致離群的行為特徵，例如因為某個特徵值過多而導致離群。如此一來，維運人員可觀察各特徵歷史資料的極端值(例如第 99 百分位數)，並將極端值視為離群值異常之判斷基準。

【0042】另外，要特別指出的是，由於信令面異常偵測機制於每小時都會匯入最新分時資料，並透過前述流程而獲得當天離群值等判定模型參數及各特徵極端值，因此在進行異常判定比對後，可立刻得到異常門號清單及其肇因。具體而言，透過上述異常樣本認定可由離群值演算法計算各特徵值的離群門檻；接著，逐一判定各特徵值是否高於離群門檻，並將符合條件之特徵列入肇因(現象)欄位中。

【0043】第 4 圖顯示本發明之訊務面異常偵測機制的流程圖。首先，定期(例如每日)匯入網路終端的訊務面歷史資料(步驟 S41)。接著，根據訊務面歷史資料重新訓練訊務面異常判定模型(步驟 S42)。繼之，使用訊務面異常判定模型預測網路終端當日的運作軌跡(步驟 S43)。另一方面，定期(例如每小時)匯入網路終端的訊務面最新分時資料(步驟 S44)。再者，透過比對預測的運作軌跡與訊務面最新分時資料，偵測網路終端是否異常(步驟 S45)。最後，可匯出異常網路終端清單(例如異常網路終端的門號清單)(步驟 S46)。

【0044】在一實施例中，考慮到訊務面資料具明顯週期性及前後期相

關性，所述訊務面異常判定模型可選擇一時間序列模型，例如整合移動平均自迴歸(ARIMA)模型。此時間序列模型能依時間變化而計算出時間點的合理訊務量，例如部分網路終端於夜間訊務量會遠低於日間訊務量，透過此時間序列模型便可分別針對不同時間點計算出適當的訊務變化。所述預測網路終端當日的運作軌跡包括預測值與信賴區間，因此，在偵測網路終端是否異常時，可透過比較預測值與實際值來加以判定。亦即，在異常偵測方面，會藉由當日預測值與最新分時資料比較的結果來判定。若實際值落於信賴區間外，則認定在此時間點之網路終端的訊務面發生異常。

【0045】第 5 圖顯示本發明之連線狀態異常偵測機制的流程圖。首先，定期(例如每日)匯入各物聯網終端群組的離線時間歷史資料(步驟 S51)。接著，使用離線時間門檻值認定模型，以決定各物聯網終端群組的離線門檻(步驟 S52)。另一方面，即時判定各物聯網終端群組中網路終端的連線狀態(步驟 S53)，若判定連線狀態為離線，則根據離線門檻判定網路終端的離線期間是否過長(步驟 S54)。最後，可匯出有離線期間過長的網路終端及離線時間之清單(步驟 S55)。

【0046】在一實施例中，上述離線時間門檻值認定模型係透過單變量分群演算法(例如 Jenks Break)來決定離線門檻。

【0047】要特別說明的是，由於各物聯網終端群組的網路終端可能存在特定短期離線或進入休眠機制的情形，因此在判定網路終端是否異常時，除了擷取其中處於離線狀態者，還要進一步從中篩選離線時間異常的網路終端。連線狀態異常偵測機制透過單變量分群演算法尋找最適切割點，並以此視為各物聯網終端群組之網路終端之離線時間門檻。這些斷點值可將離線時間分佈合理切割，並將離線時間分別為不同群聚，再從群聚之離線時間中選擇一者作為合理的離線時間門檻值。獲得離線時間門檻值後，即

時偵測到離線的網路終端，便可透過此機制進行篩選。亦即，有離線時間大於離線時間門檻值(例如 300 分鐘)的網路終端，將被視為連線狀態異常。

【0048】第 6 圖顯示本發明之細胞面資料分析機制的流程圖。首先，定期(例如每日)進行駐留細胞判定(步驟 S61)，其中透過選取網路終端連線最頻繁之細胞，且細胞在最近一段期間內(例如最近數日)所連線之網路終端數目超過一預定門檻將被認定為駐留細胞，並產生駐留細胞清單(步驟 S62)。亦即，透過分析細胞連線數，以將連線人數過少之細胞濾除。另一方面，定期(例如每小時)匯入行動網路之信令面資料、訊務面資料及各網路終端之連線狀態資料(步驟 S63)，並篩選與駐留細胞相關的資料(步驟 S64)。接著，可分別由信令面、訊務面與連線狀態來判定各駐留細胞是否異常(步驟 S65)。

【0049】要特別說明的是，由信令面、訊務面與連線狀態來判定各駐留細胞是否異常時，可採用前述信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制所揭示的相關流程來進行。如第 6 圖所示，可對篩選後與駐留細胞相關的資料，依細胞、時間加總信令面資料(步驟 S651)，而得到各駐留細胞的信令面資料；或是取各細胞之分時訊務面資料之中位數或百分位數為代表(步驟 S652)，而得到各駐留細胞之訊務面資料之分時趨勢估計。接著，分別對信令面資料、訊務面資料及各駐留細胞連線相關之網路終端之狀態資料，執行信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制的相關流程。又，執行信令面異常偵測機制(步驟 S653)，可產生異常細胞清單(步驟 S654)；執行訊務面異常偵測機制(步驟 S655)，可產生細胞特徵軌跡及相關告警(步驟 S656)；執行連線狀態異常偵測機制(步驟 S657)，可產生異常細胞之離線門檻(步驟 S658)，並產生離線細胞、離線時間之清單(步驟 S659)。

【0050】第 7 圖顯示本發明之物聯網終端群組面資料分析機制的流程圖。首先，定期(例如每日)進行活躍門號判定(步驟 S71)，以將各物聯網終端群組中最近一段期間內(例如最近數日)曾上線之網路終端設定為活躍網路終端，再根據活躍網路終端產生活躍門號清單(步驟 S72)。亦即，透過篩選最近數日內曾上線的網路終端來進行分析，可避免物聯網終端群組的總體指標受到下線的網路終端所影響。另一方面，定期(例如每小時)匯入行動網路之信令面資料、訊務面資料及各網路終端之連線狀態資料(步驟 S73)，並篩選與活躍網路終端相關的資料(步驟 S74)。接著，可分別由信令面、訊務面與連線狀態來判斷各物聯網終端群組是否異常(步驟 S75)。

【0051】同樣的，由信令面、訊務面與連線狀態來判定各物聯網終端群組是否異常時，亦可採用前述信令面異常偵測機制與訊務面異常偵測機制的相關流程來進行。如第 7 圖所示，可對篩選後活躍網路終端的相關資料，依物聯網終端群組、時間加總信令面資料(步驟 S751)，而得到各活躍網路終端的信令面資料；或是取各物聯網終端群組之分時訊務面資料之中位數或百分位數為代表(步驟 S752)，而得到各活躍網路終端之訊務面資料之分時趨勢估計。接著，分別對所得到之信令面資料、訊務面資料之分時趨勢估計及各活躍網路終端之連線狀態資料，執行信令面異常偵測機制與訊務面異常偵測機制等相關流程。又，執行信令面異常偵測機制(步驟 S753)，可產生異常物聯網終端群組清單(步驟 S754)；執行訊務面異常偵測機制(步驟 S755)，可產生物聯網終端群組之特徵軌跡及相關告警(步驟 S756)；透過時間序列模型分析各物聯網終端群組之連線數趨勢，以判斷連線數是否異常(步驟 S757)，並產生有連線異常之物聯網終端群組之時間點(步驟 S758)。

【0052】值得注意的是，針對物聯網終端群組之連線狀態的偵測，可

透過定時紀錄各物聯網終端群組之網路終端的上線門號數，並嘗試針對上線門號過少之時間點提出告警。由於各物聯網終端群組存在不同上線行為，且具一定程度周期性、前後期相關性，因此本發明採用訊務面異常偵測機制，透過時間序列模型估計各物聯網終端群組之時間點合理上線數範圍，並以此作為物聯網終端群組之各時段連線數異常值的認定基準。

【0053】第 8 圖顯示本發明之基於行動物聯網之網路行為異常偵測方法的流程圖，且此方法主要包括下列步驟，其餘內容相同於上述第 1 圖至第 7 圖之說明，於此不再重覆敘述。首先，擷取行動網路之信令面資料、訊務面資料與連線狀態資料(步驟 S81)。接著，使用離群值演算法處理信令面資料，以偵測行動網路之信令面是否異常(步驟 S82)。繼之，使用時間序列模型處理訊務面資料並進行預測，以判定行動網路之訊務面是否異常(步驟 S83)。然後，使用單變量分群演算法處理連線狀態資料，以偵測行動網路之連線狀態是否異常(步驟 S84)。

【0054】在一實施例中，上述網路行為異常偵測方法更包括下列步驟。首先，進行駐留細胞判定(步驟 S851)。接著，篩選屬於駐留細胞的信令面資料、訊務面資料與連線狀態資料(步驟 S852)。最後，分別由信令面、訊務面與連線狀態來判定駐留細胞是否異常(步驟 S853)。

【0055】在一實施例中，上述網路行為異常偵測方法更包括下列步驟。首先，從各物聯網終端群組中找出近期曾連線之網路終端(步驟 S861)。接著，篩選與網路終端相關的信令面資料、訊務面資料與連線狀態資料(步驟 S862)。最後，分別由信令面、訊務面與連線狀態來判斷各物聯網終端群組是否異常(步驟 S863)。

【0056】本發明之基於行動物聯網之網路行為異常偵測系統及方法係至少具有下列優點或技術功效。

【0057】首先，透過收集行動網路資料，將終端與局端之間的連線行為，以時間序列、離群值等人工智慧演算法建構出物聯網終端異常行為偵測模型，因此能有效的分析行動物聯網之全體終端的實際使用狀況，且可以無須如習知技術般在各終端進行觀測。又，即使當任意的物聯網終端損壞而斷線失聯，亦能透過本發明之偵測模型在第一時間偵測發現異常，不影響運作性能。

【0058】再者，本發明的信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制，可分別針對信令、流量與連線狀態進行全面的異常行為偵測，且相關的偵測機制全程自動化，因此能有效提升維運大量物聯網終端的效率。

【0059】另外，由於本發明的訓練模型導入了移動窗格的概念，可定期(例如日或每小時)依照最新收集到的資料來調整偵測模型，因此能充分且有效的因應物聯網終端行為的變化趨勢。

【0060】上述實施例僅為例示性說明本發明之技術原理、特點及其功效，並非用以限制本發明之可實施範疇，任何熟習此技術之人士均可在不違背本發明之精神與範疇下，對上述實施形態進行修飾與改變。然任何運用本發明所教示內容而完成之等效修飾及改變，均仍應為所附之申請專利範圍所涵蓋。而本發明之權利保護範圍，應如所附之申請專利範圍所列。

【符號說明】

【0061】

1	網路行為異常偵測系統
10	網路特徵收集模組
101	信令面資料

102 訊務面資料

103 連線狀態資料

11 網路終端異常偵測模組

111 信令面異常偵測機制

112 訊務面異常偵測機制

113 連線狀態異常偵測機制

12 網路拓樸異常偵測模組

121 細胞面資料分析機制

122 物聯網終端群組面資料分析機制

13 維運查詢介面

14 維運端

S21 至 S26、S31 至 S35 步驟

S41 至 S46、S51 至 S55 步驟

S61 至 S65、S651 至 S659 步驟

S71 至 S75、S751 至 S758 步驟

S81 至 S84、S851 至 S853 步驟

S861 至 S863 步驟

第 108144919 號專利申請案
109 年 12 月 24 日修正替換頁

【發明申請專利範圍】

【第1項】 一種基於行動物聯網之網路行為異常偵測系統，包括：

網路終端異常偵測模組，係具有信令面異常偵測機制、訊務面異常偵測機制與連線狀態異常偵測機制，以分別偵測網路終端之信令面、訊務面與連線狀態三者之異常；以及

網路拓樸異常偵測模組，係具有細胞面資料分析機制與物聯網終端群組面資料分析機制，以分別偵測細胞與物聯網終端群組二者之異常，

其中，該網路行為異常偵測系統使用離群值演算法處理行動網路之信令面資料以偵測該行動網路之信令面是否異常，使用整合移動平均自迴歸(ARIMA)模型處理該行動網路之訊務面資料並進行預測以判定該行動網路之訊務面是否異常，且使用單變量分群演算法處理該行動網路之連線狀態資料以偵測該行動網路之連線狀態是否異常。

【第2項】 如申請專利範圍第 1 項所述之網路行為異常偵測系統，更包括一網路特徵收集模組，用以收集該行動網路之信令面資料、訊務面資料與連線狀態資料，並對該信令面資料、該訊務面資料與該連線狀態資料進行彙整與預處理。

【第3項】 如申請專利範圍第 2 項所述之網路行為異常偵測系統，其中，該網路特徵收集模組係執行下列程序：

判斷是否有該網路終端之歷史資料，若無該歷史資料，則進行歷史分時資料收集，以取得預定期間內該行動網路之該信令面資料、該訊務面資料與網路終端離線時間；

收集最新分時資料，以取得該行動網路之該信令面資料與該訊務面資料；以及

對該歷史分時資料與該最新分時資料進行彙整與預處理，且更新該歷史資料。

【第4項】 如申請專利範圍第 1 項所述之網路行為異常偵測系統，其中，該網路終端異常偵測模組之該信令面異常偵測機制係包括下列程序：

定期匯入該網路終端的信令面歷史資料，根據該信令面歷史資料重新訓練信令面異常判定模型以更新模型參數；

匯入該網路終端的信令面最新分時資料；

使用該信令面異常判定模型進行異常判定；以及

匯出異常網路終端清單。

【第5項】 如申請專利範圍第 4 項所述之網路行為異常偵測系統，其中，該信令面異常判定模型係用以進行異常樣本認定與異常肇因推測，且其中，該異常樣本認定是透過離群值判定演算法來認定，而該異常肇因推測是彙整與記錄導致離群的行為特徵。

【第6項】 如申請專利範圍第 1 項所述之網路行為異常偵測系統，其中，該網路終端異常偵測模組之該訊務面異常偵測機制包括下列程序：

定期匯入該網路終端的訊務面歷史資料；

根據該訊務面歷史資料重新訓練為該整合移動平均自迴歸(ARIMA)模型之訊務面異常判定模型；

使用該訊務面異常判定模型，預測該網路終端當日的運作軌跡；

匯入該網路終端的訊務面最新分時資料；

第 108144919 號專利申請案
109 年 12 月 24 日修正替換頁

偵測該網路終端是否異常；以及

匯出異常網路終端清單。

【第7項】 如申請專利範圍第 6 項所述之網路行為異常偵測系統，其中，所述預測該網路終端當日的運作軌跡包括預測值與信賴區間，且所述偵測該網路終端是否異常係透過比較該預測值與實際值而判定。

【第8項】 如申請專利範圍第 1 項所述之網路行為異常偵測系統，其中，該網路終端異常偵測模組之該連線狀態異常偵測機制係包括下列程序：

匯入各物聯網終端群組的離線時間歷史資料；

使用一離線時間門檻值認定模型決定各該物聯網終端群組的離線門檻；

即時判定各該物聯網終端群組中該網路終端的連線狀態，若判定該連線狀態為離線，則根據該離線門檻判定該網路終端的離線期間是否過長；以及

匯出有離線期間過長之該網路終端及其離線時間。

【第9項】 如申請專利範圍第 8 項所述之網路行為異常偵測系統，其中，該離線時間門檻值認定模型係透過該單變量分群演算法來決定該離線門檻。

【第10項】 如申請專利範圍第 1 項所述之網路行為異常偵測系統，其中，該網路拓樸異常偵測模組之該細胞面資料分析機制包括下列程序：

進行駐留細胞判定，其中，透過選取該網路終端連線最頻繁之細胞，且該細胞在最近一段期間內所連線之該網路終端數目超過一預定門檻而認定該細胞為駐留細胞；

匯入該行動網路之信令面資料、訊務面資料及各該網路終端之連線狀態資料，並篩選與該駐留細胞相關的資料；以及

第 108144919 號專利申請案
109 年 12 月 24 日修正替換頁

分別由信令面、訊務面與連線狀態來判定各該駐留細胞是否異常。

【第11項】 如申請專利範圍第 1 項所述之網路行為異常偵測系統，其中，該網路拓樸異常偵測模組之該物聯網終端群組面資料分析機制包括下列程序：

將各該物聯網終端群組中最近一段期間內曾上線之該網路終端設定為活躍網路終端；

匯入該行動網路之信令面資料、訊務面資料及各該網路終端之連線狀態資料，並篩選與該活躍網路終端相關的資料；以及

分別由信令面、訊務面與連線狀態來判斷各該物聯網終端群組是否異常。

【第12項】 一種基於行動物聯網之網路行為異常偵測方法，包括：

擷取行動網路之信令面資料、訊務面資料與連線狀態資料；

使用離群值演算法處理該行動網路之信令面資料，以偵測該行動網路之信令面是否異常；

使用整合移動平均自迴歸(ARIMA)模型處理該行動網路之訊務面資料並進行預測，以判定該行動網路之訊務面是否異常；以及

使用單變量分群演算法處理該行動網路之連線狀態資料，以偵測該行動網路之連線狀態是否異常。

【第13項】 如申請專利範圍第 12 項所述之網路行為異常偵測方法，更包括：

進行駐留細胞判定；

篩選屬於該駐留細胞的該信令面資料、該訊務面資料與該連線狀態資料；以及

分別由信令面、訊務面與連線狀態來判定該駐留細胞是否異常。

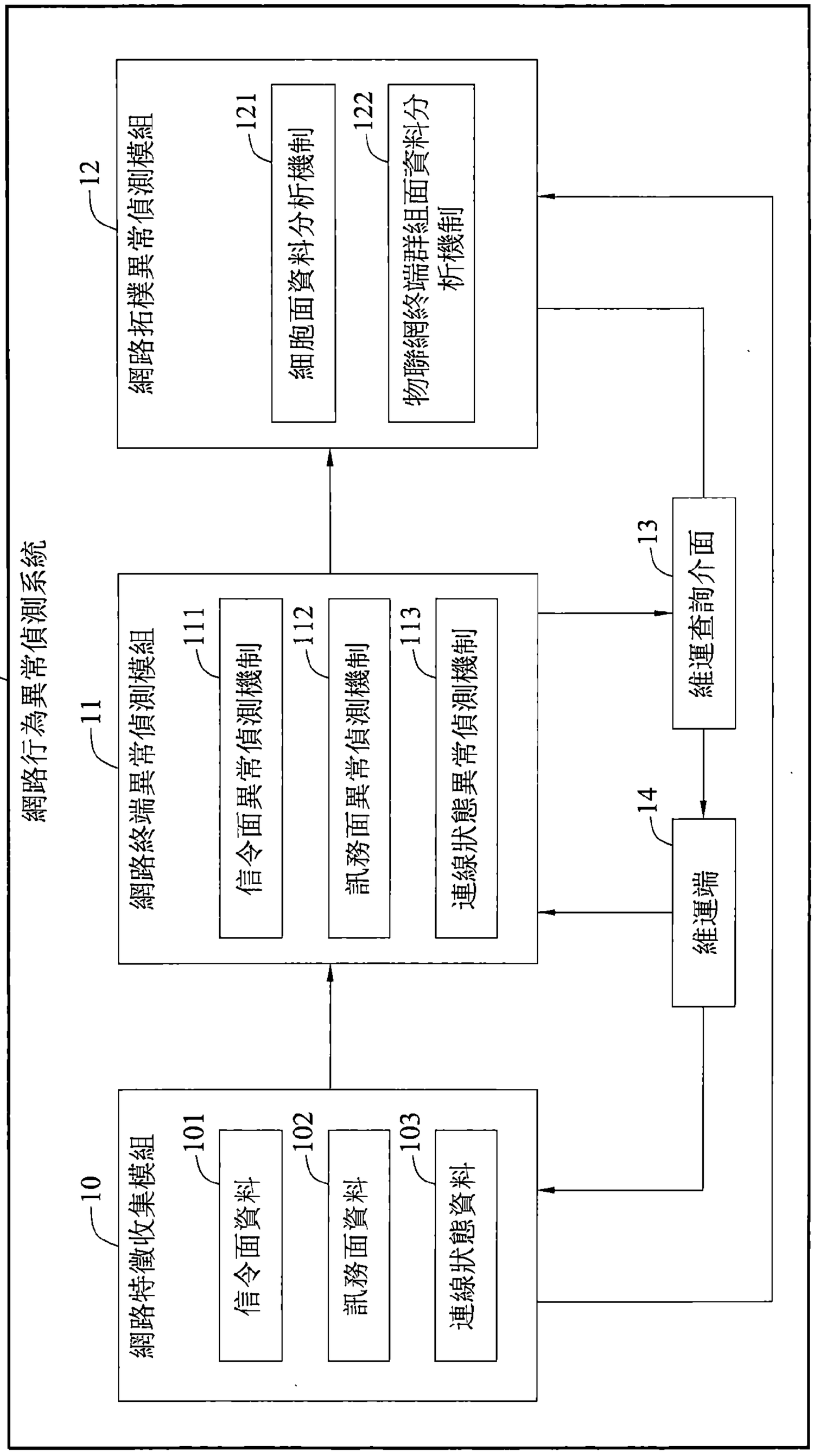
【第14項】 如申請專利範圍第 12 項所述之網路行為異常偵測方法，更包括：

從各物聯網終端群組中找出近期曾連線之網路終端；

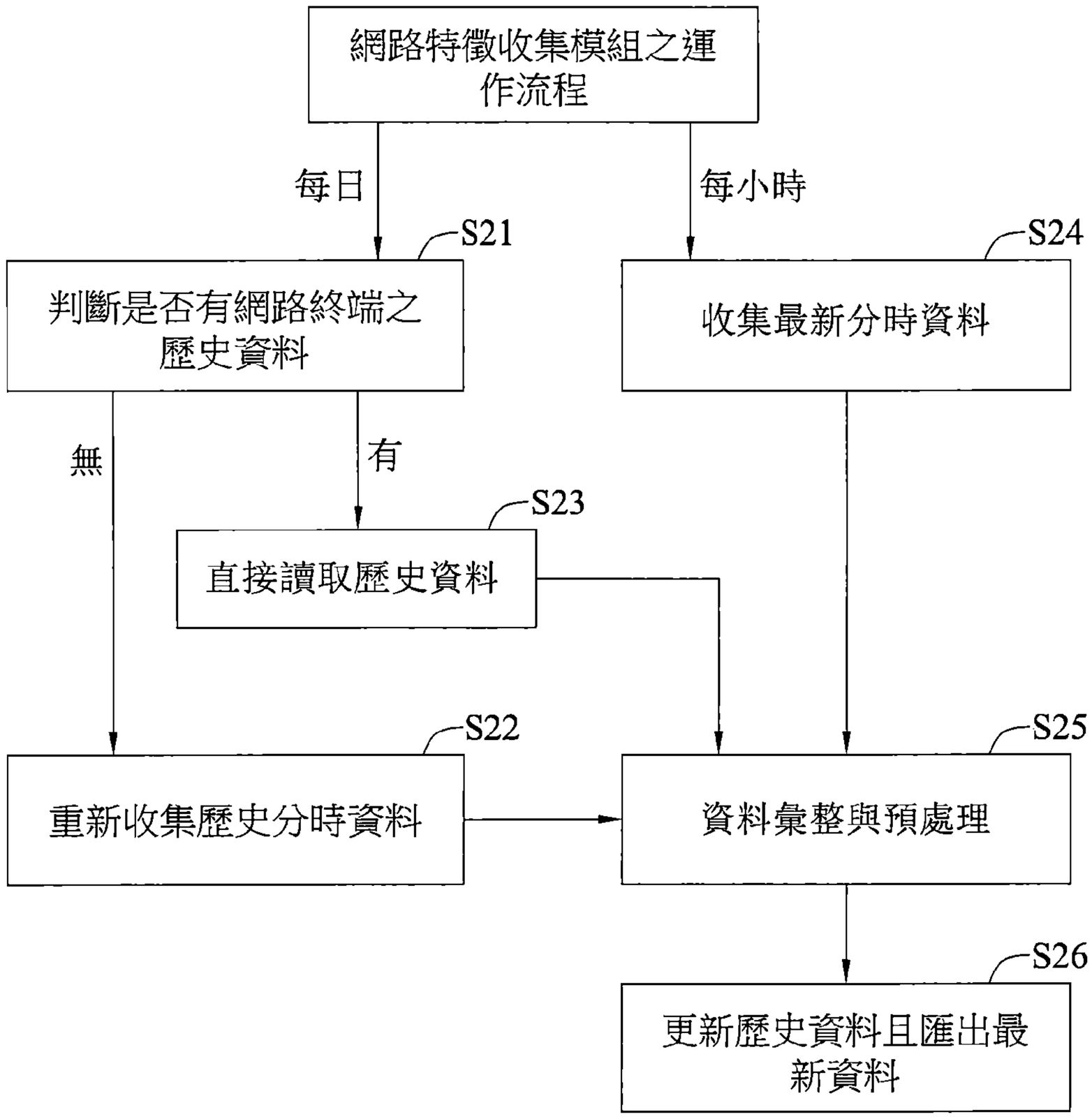
篩選與該網路終端相關的該信令面資料、該訊務面資料與該連線狀態資料；以及

分別由信令面、訊務面與連線狀態來判斷各該物聯網終端群組是否異常。

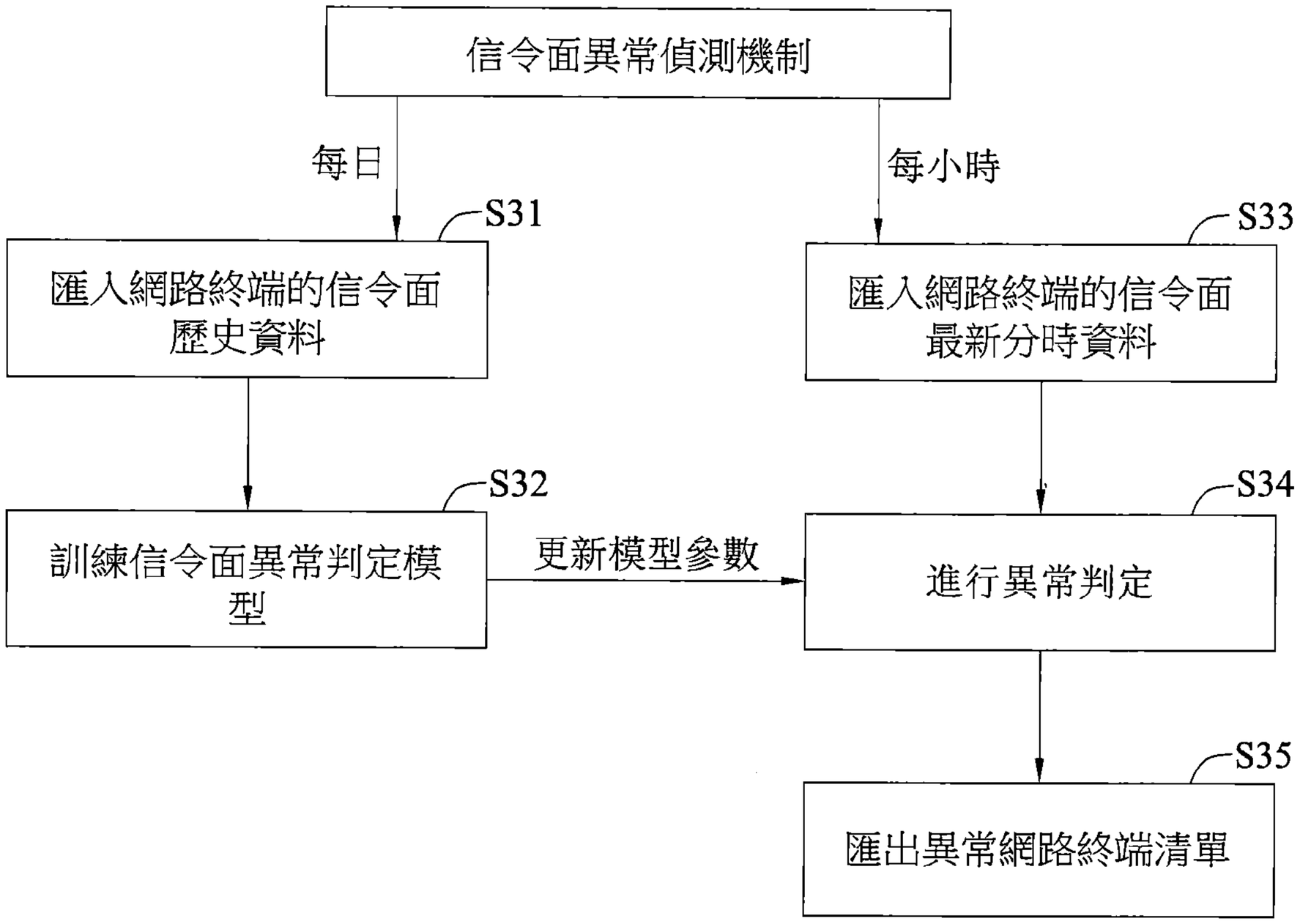
【發明圖式】


1
網路行為異常偵測系統
12
網路拓樸異常偵測模組
121
細胞面資料分析機制
122
物聯網終端群組面資料分析機制
11
網路終端異常偵測模組
111
信令面異常偵測機制
112
訊務面異常偵測機制
113
連線狀態異常偵測機制
13
維運查詢介面
14
維運端
10
網路特徵收集模組
101
信令面資料
102
訊務面資料
103
連線狀態資料

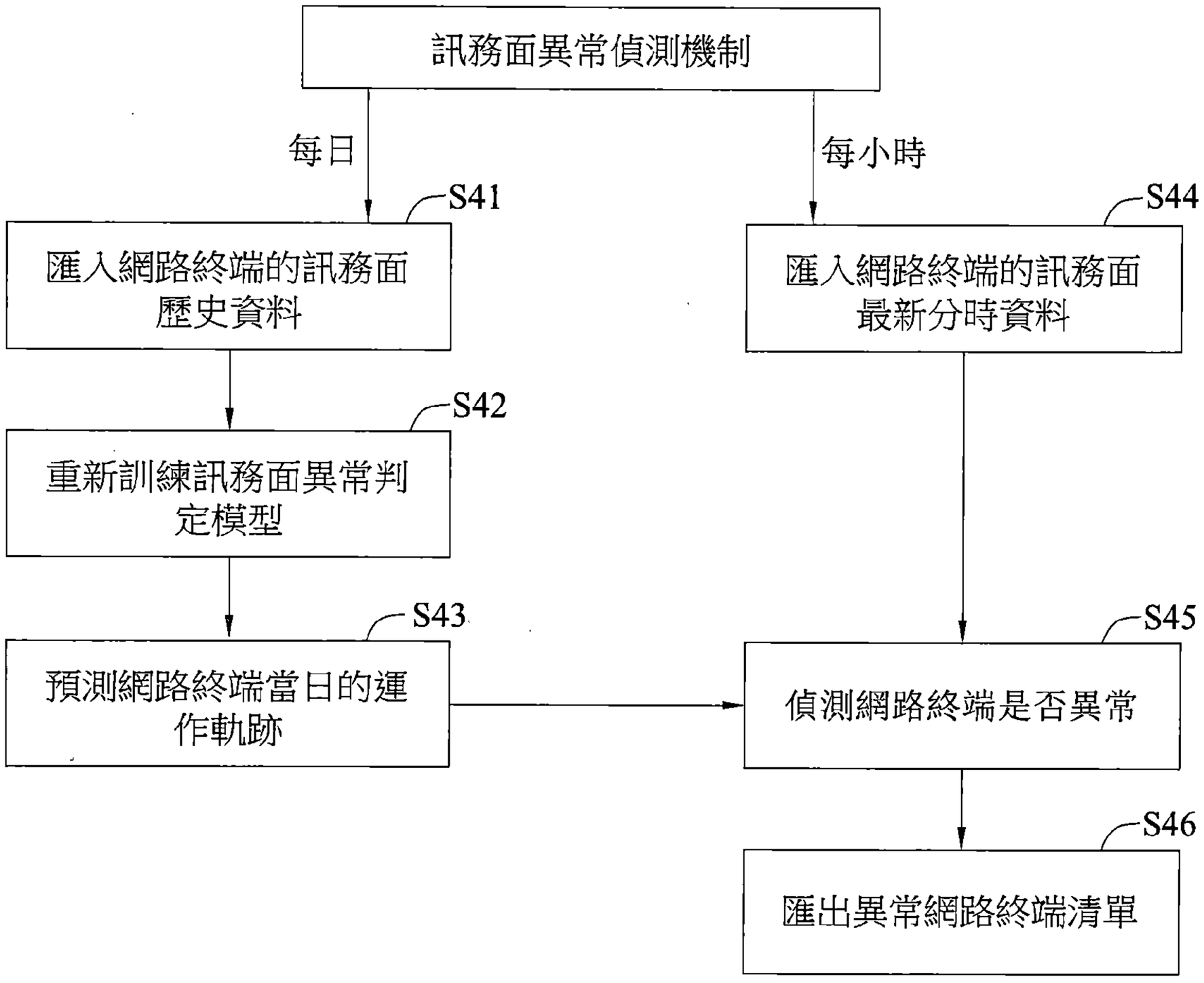
【第1圖】


網路特徵收集模組之運作流程
每日
每小時
S21
判斷是否有網路終端之歷史資料
S24
收集最新分時資料
無
有
S23
直接讀取歷史資料
S22
重新收集歷史分時資料
S25
資料彙整與預處理
S26
更新歷史資料且匯出最新資料

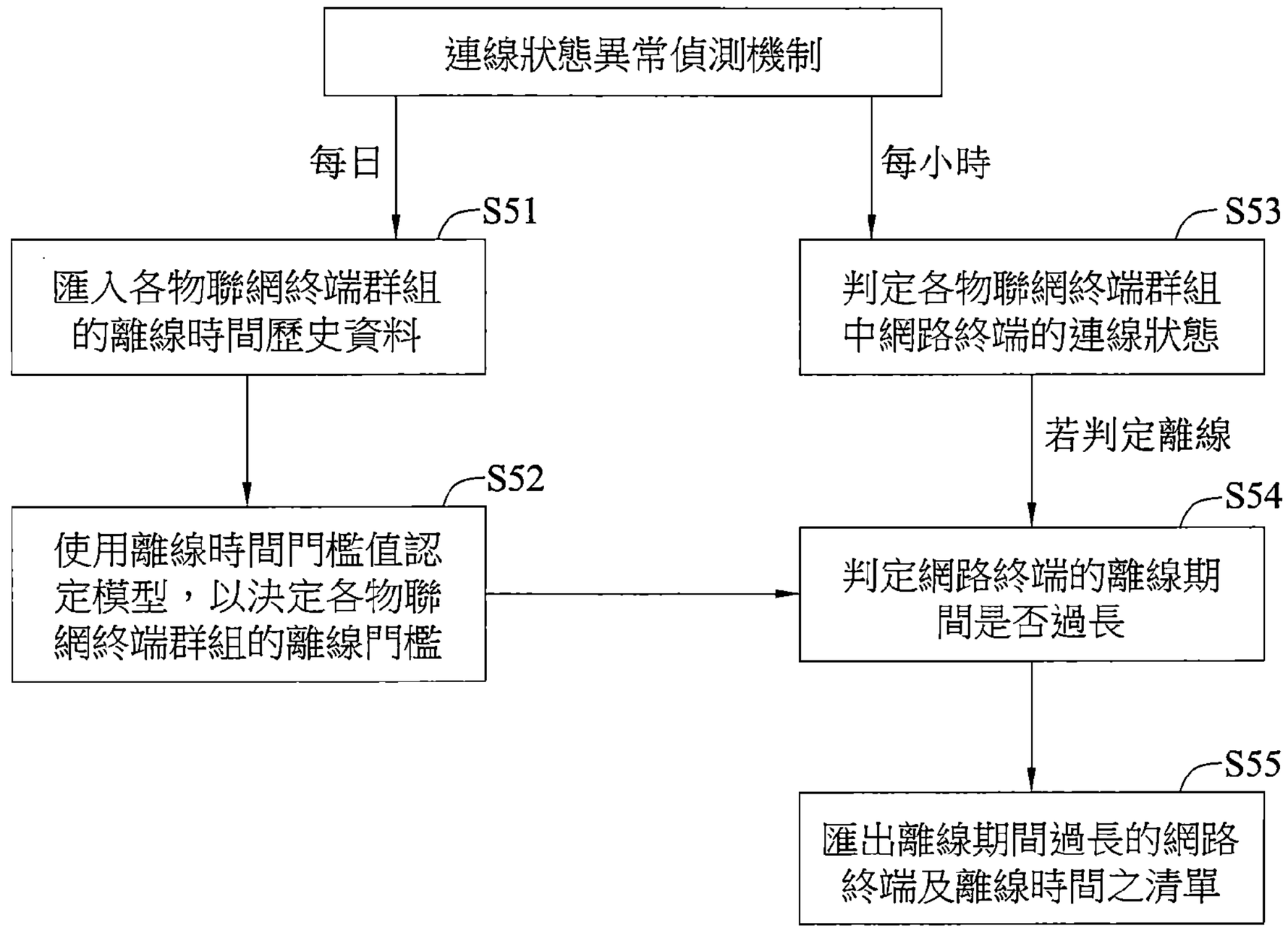
【第2圖】


信令面異常偵測機制
每日
每小時
S31
匯入網路終端的信令面歷史資料
S33
匯入網路終端的信令面最新分時資料
S32
訓練信令面異常判定模型
更新模型參數
S34
進行異常判定
S35
匯出異常網路終端清單

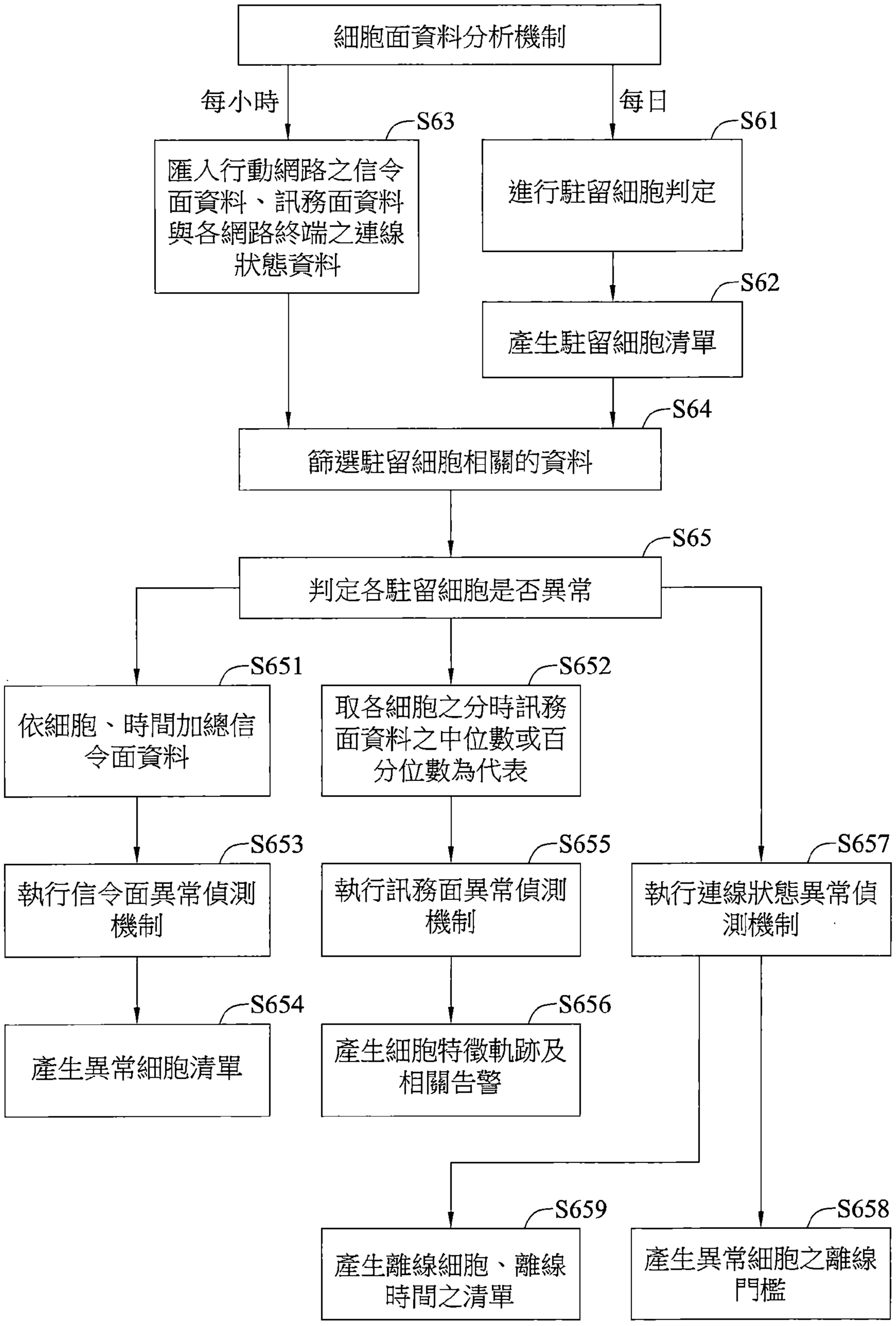
【第3圖】


訊務面異常偵測機制
每日
每小時
S41
匯入網路終端的訊務面歷史資料
S42
重新訓練訊務面異常判定模型
S43
預測網路終端當日的運作軌跡
S44
匯入網路終端的訊務面最新分時資料
S45
偵測網路終端是否異常
S46
匯出異常網路終端清單

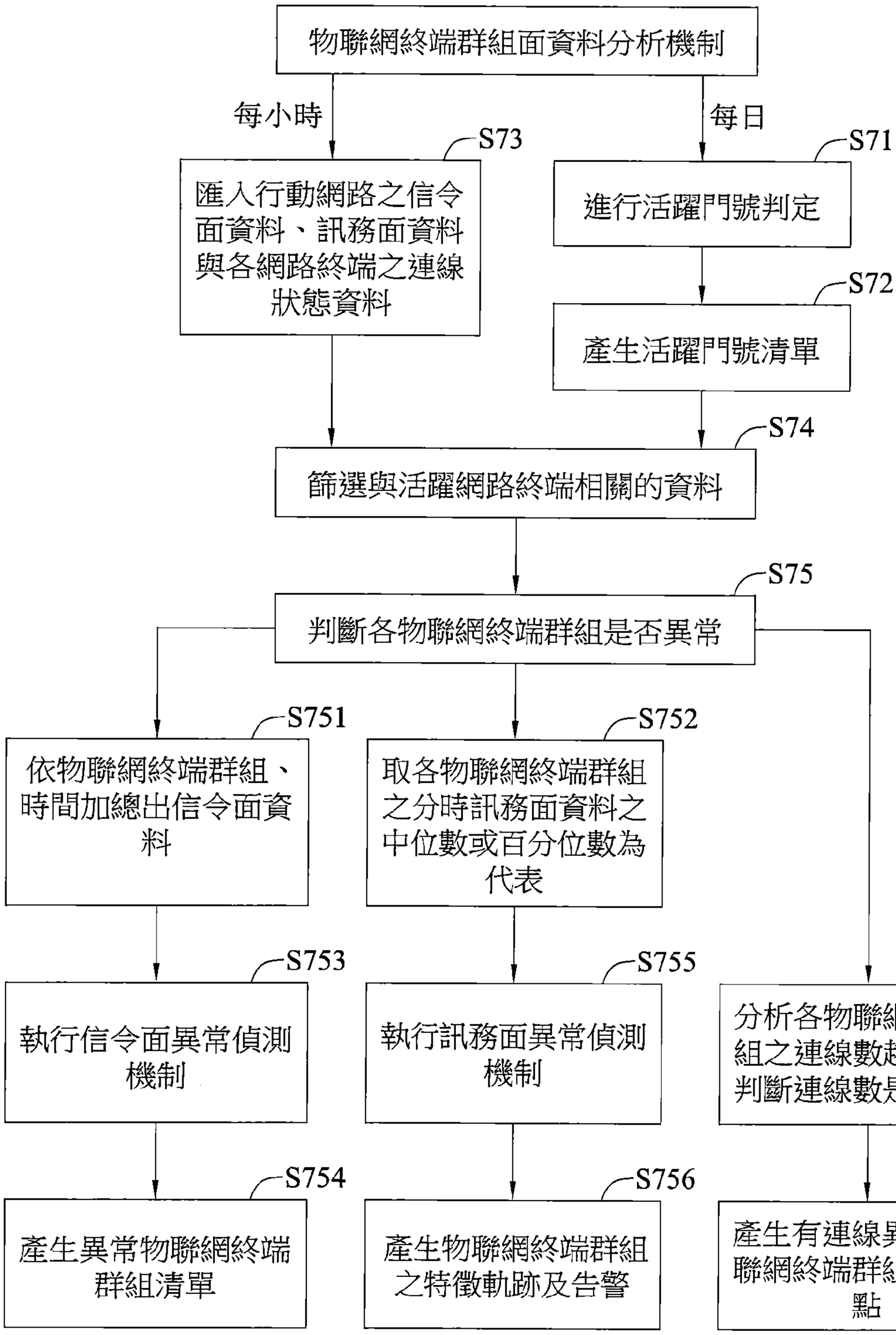
【第4圖】


連線狀態異常偵測機制
每日
每小時
S51
匯入各物聯網終端群組的離線時間歷史資料
S52
使用離線時間門檻值認定模型，以決定各物聯網終端群組的離線門檻
S53
判定各物聯網終端群組中網路終端的連線狀態
若判定離線
S54
判定網路終端的離線期間是否過長
S55
匯出離線期間過長的網路終端及離線時間之清單

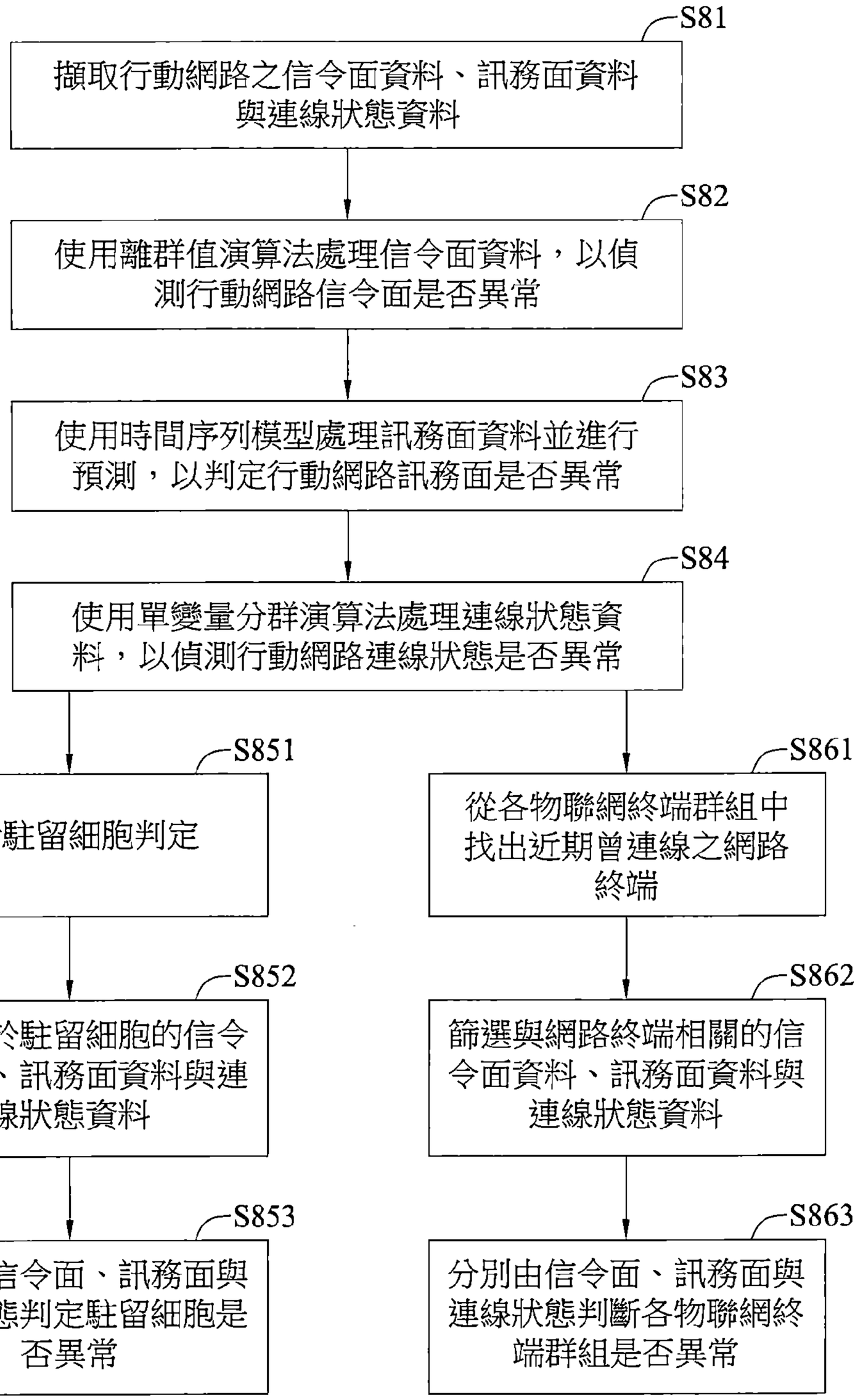
【第5圖】


細胞面資料分析機制
每小時
每日
S63
S61
匯入行動網路之信令面資料、訊務面資料與各網路終端之連線狀態資料
進行駐留細胞判定
S62
產生駐留細胞清單
S64
篩選駐留細胞相關的資料
S65
判定各駐留細胞是否異常
S651
S652
依細胞、時間加總信令面資料
取各細胞之分時訊務面資料之中位數或百分位數為代表
S653
S655
S657
執行信令面異常偵測機制
執行訊務面異常偵測機制
執行連線狀態異常偵測機制
S654
S656
產生異常細胞清單
產生細胞特徵軌跡及相關告警
S659
S658
產生離線細胞、離線時間之清單
產生異常細胞之離線門檻

【第6圖】


物聯網終端群組面資料分析機制
每小時
每日
S73
S71
匯入行動網路之信令面資料、訊務面資料與各網路終端之連線狀態資料
進行活躍門號判定
S72
產生活躍門號清單
S74
篩選與活躍網路終端相關的資料
S75
判斷各物聯網終端群組是否異常
S751
S752
依物聯網終端群組、時間加總出信令面資料
取各物聯網終端群組之分時訊務面資料之中位數或百分位數為代表
S753
S755
S757
執行信令面異常偵測機制
執行訊務面異常偵測機制
分析各物聯網終端群組之連線數趨勢，以判斷連線數是否異常
S754
S756
S758
產生異常物聯網終端群組清單
產生物聯網終端群組之特徵軌跡及告警
產生有連線異常之物聯網終端群組之時間點

【第7圖】


S81
擷取行動網路之信令面資料、訊務面資料與連線狀態資料
S82
使用離群值演算法處理信令面資料，以偵測行動網路信令面是否異常
S83
使用時間序列模型處理訊務面資料並進行預測，以判定行動網路訊務面是否異常
S84
使用單變量分群演算法處理連線狀態資料，以偵測行動網路連線狀態是否異常
S851
進行駐留細胞判定
S852
篩選屬於駐留細胞的信令面資料、訊務面資料與連線狀態資料
S853
分別由信令面、訊務面與連線狀態判定駐留細胞是否異常
S861
從各物聯網終端群組中找出近期曾連線之網路終端
S862
篩選與網路終端相關的信令面資料、訊務面資料與連線狀態資料
S863
分別由信令面、訊務面與連線狀態判斷各物聯網終端群組是否異常

【第8圖】