I405434

(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 I405434B1**

(45)公告日： 中華民國 102 (2013) 年 08 月 11 日

(21)申請案號：098122517 (22)申請日： 中華民國 98 (2009) 年 07 月 03 日

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

(71)申請人：國立臺灣科技大學 (中華民國) NATIONAL TAIWAN UNIVERSITY OF SCIENCE AND TECHNOLOGY (TW)
臺北市大安區基隆路 4 段 43 號

(72)發明人：李漢銘 LEE, HAHN MING (TW)；毛敬豪 MAO, CHING HAO (TW)；陳裕傑 CHEN, YU JIE (TW)；王奕勛 WANG, YI HSUN (TW)；葉治宏 YEH, JE ROME (TW)；陳祖翰 CHEN, TSUHAN CHEN (TW)

(74)代理人：洪澄文；顏錦順

(56)參考文獻：

TW 200702988 TW 200912682

US 6622150B1

審查人員：陳雍宗

申請專利範圍項數：18 項 圖式數：4 共 0 頁

(54)名稱

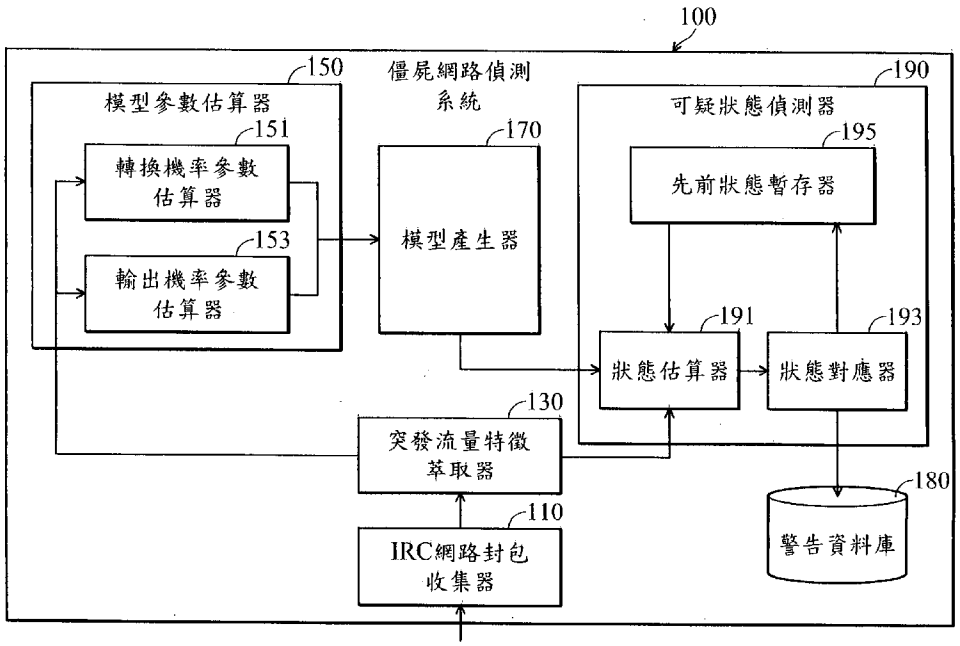
殭屍網路偵測系統及方法

BOTNET EARLY DETECTION USING HHMM ALGORITHM

(57)摘要

一種僵屍網路偵測系統，其包括：一突發流量特徵萃取器，接收一偵測對象網路中一網際網路中繼聊天(IRC)封包的欄位值，並據以計算一突發流量特徵值；一模型參數估算器，依據該突發流量特徵值，決定混合隱藏式馬可夫模型(Hybrid Hidden Markov Model,HHMM)所需之機率參數值；一模型產生器，依據該機率參數值，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型；及一可疑狀態偵測器，當接收到一新的 IRC 封包，並由突發流量特徵萃取器據以產生突發流量特徵值之後，該可疑狀態偵測器將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型中，據以判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生相對的警告訊息。

A botnet detection system is provided. A bursty feature extractor receives an IRC packet value of a detected network, and determines a bursty feature accordingly. A HHMM parameter estimator determines parameters for a Hybrid Hidden Markov Model according to the bursty feature. A traffic profile generator models and profiles network traffic. When a new IRC packet is received and its bursty feature is determined, a state estimator determines a traffic state corresponding to a network relaying the IRC packet, and determines whether the network is a botnet.



第 1 圖

100・・・僵屍網路偵測系統

110・・・IRC 網路封包收集器

130・・・突發流量特徵萃取器

150・・・模型參數估算器

151・・・轉換機率參數估算器

153・・・輸出機率參數估算器

170・・・模型產生器

190・・・可疑狀態偵測器

191・・・狀態估算器

193・・・狀態對應器

195・・・先前狀態暫存器

180・・・警告資料庫

I405434

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：098122517

※ 申請日：98.7.3　※IPC 分類：H04L 12/26 (2006.01)

一、發明名稱：（中文/英文）

殭屍網路偵測系統及方法

Botnet Early Detection Using HHMM Algorithm

二、中文發明摘要：

一種僵屍網路偵測系統，其包括：一突發流量特徵萃取器，接收一偵測對象網路中一網際網路中繼聊天（IRC）封包的欄位值，並據以計算一突發流量特徵值；一模型參數估算器，依據該突發流量特徵值，決定混合隱藏式馬可夫模型（Hybrid Hidden Markov Model, HHMM）所需之機率參數值；一模型產生器，依據該機率參數值，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型；及一可疑狀態偵測器，當接收到一新的IRC 封包，並由突發流量特徵萃取器據以產生突發流量特徵值之後，該可疑狀態偵測器將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型中，據以判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生相對的警告訊息。

三、英文發明摘要：

A botnet detection system is provided. A bursty feature extractor receives an IRC packet value of a detected

network, and determines a bursty feature accordingly. A HHMM parameter estimator determines parameters for a Hybrid Hidden Markov Model according to the bursty feature. A traffic profile generator models and profiles network traffic. When a new IRC packet is received and its bursty feature is determined, a state estimator determines a traffic state corresponding to a network relaying the IRC packet, and determines whether the network is a botnet.

四、指定代表圖：

(一)本案指定代表圖為：第（1）圖。

(二)本代表圖之元件符號簡單說明：

僵屍網路偵測系統 100

IRC 網路封包收集器 110

突發流量特徵萃取器 130

模型參數估算器 150

轉換機率參數估算器 151

輸出機率參數估算器 153

模型產生器 170

可疑狀態偵測器 190

狀態估算器 191

狀態對應器 193

先前狀態暫存器 195

警告資料庫 180

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。

六、發明說明：

【發明所屬之技術領域】

本發明係有關於一種電腦系統與方法，特別是有關於一種偵測僵屍網路（botnet）的電腦系統與方法。

【先前技術】

近年來，用於從事惡意目的的殭屍網路 (botnet) 活動數量正與日俱增。不法的殭屍操控者 (Botmaster) 可從他處集中操控殭屍程式，下指令啟動殭屍程式 (bot) 來執行大規模的惡意活動，包括散佈垃圾郵件、網路釣魚、阻絕服務程式 (DoS) 攻擊及勒索威脅。

傳統上用以偵測僵屍網路的方法，多半依賴已知的病毒碼，且無法早期偵測到僵屍網路。

因此，需要一種能夠有效偵測僵屍網路的系統與方法。

【發明內容】

本發明提供一種僵屍網路偵測系統，其包括：一突發流量特徵萃取器，接收一偵測對象網路中一網際網路中繼聊天（IRC）封包的欄位值，並據以計算一突發流量特徵值；一模型參數估算器，依據該突發流量特徵值，決定混合隱藏式馬可夫模型（Hybrid Hidden Markov Model, HHMM）所需之機率參數值；一模型產生器，依據該機率參數值，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型；及一可疑狀態偵測器，當接收到一新的 IRC 封包，並由突發流量特徵萃取器據以產生突發流量特徵值之後，該可疑狀態偵測器將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型中，據以

判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生相對的警告訊息。

本發明另提供一種殭屍網路偵測方法，其包括：接收一偵測對象網路中一網際網路中繼聊天（IRC）封包的欄位值，並據以計算一突發流量特徵值；依據該突發流量特徵值，決定混合隱藏式馬可夫模型（Hybrid Hidden Markov Model, HHMM）所需之機率參數值；依據該機率參數值，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型；及當接收到一新的 IRC 封包，並由突發流量特徵萃取器據以產生突發流量特徵值之後，該可疑狀態偵測器將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型中，據以判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生相對的警告訊息。

為讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉出較佳實施例，並配合所附圖式，作詳細說明如下：

【實施方式】

第 1 圖顯示依據本發明實施例之僵屍網路偵測系統之方塊圖。

如第 1 圖所示，僵屍網路偵測系統 100 主要包括：一 IRC 網路封包收集器 110、一突發流量特徵萃取器 130、一模型參數估算器 150、一模型產生器 170、一可疑狀態偵測器 190、及一警告資料庫 180。

IRC 網路封包收集器 110 從網路收集封包，並篩選出網際網路中繼聊天(Internet Relay Chat, IRC)封包，擷取並

輸出該 IRC 封包的欄位值。

突發流量特徵萃取器 130 接收該 IRC 封包的欄位值，並據以計算突發流量特徵值。在此，突發流量特徵值有二：其一為每秒鐘封包大小的平均值，另一則是每秒鐘封包間隔時間的平均值。

模型參數估算器 150，依據該突發流量特徵值，決定混合隱藏式馬可夫模型（Hybrid Hidden Markov Model, HHMM）所需之機率參數值，亦即轉換機率（transition probability）參數及輸出機率（emission probability）參數。

模型參數估算器 150 包括轉換機率參數估算器 151 及輸出機率參數估算器 153。

其中，轉換機率參數估算器 151 依據該突發流量特徵值，計算各個預先定義的狀態間轉換機率，以產生轉換機率參數。轉換機率參數估算器 151 利用條件機率配合統計的計次法則(Counting rule)，依序計算每一筆訓練資料(Instance)所屬的行為狀態類別在整個訓練資料集(Training set)中所佔有的比率，該比率便是該筆資料的轉換機率。

輸出機率參數估算器 153 依據該突發流量特徵值，計算該流量突發特徵值符合各個預先定義狀態的可能機率，以產生該輸出機率參數。輸出機率參數估算器 153 利用條件機率配合統計的計次法則，計算每一個訓練資料中萃取出的特徵向量值在行為狀態中的機率。

模型產生器 170 依據該轉換機率參數及該輸出機率參數，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型，供後續用於偵測殭屍網路所產生的異常流量。在此，預先定義了三種網路行為狀態

類別：正常行為狀態(Normal state)、閒置行為狀態(Idle state)和動作行為狀態(Active state)。

模型參數估算器 150 及模型產生器 170 係在訓練階段運作，由收集到的 IRC 封包產生混合隱藏式馬可夫模型之機率時序模型，以供後續偵測僵屍網路之用。

當突發流量特徵萃取器 130 從一偵測對象網路接收到 IRC 封包，並由突發流量特徵萃取器 130 據以產生突發流量特徵值之後，由可疑狀態偵測器 190 將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型，判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生並儲存相對的警告訊息。

可疑狀態偵測器 190 包括一狀態估算器 191、狀態對應器 193 及先前狀態暫存器 195。

狀態估算器 191 依據突發流量特徵萃取器 130 輸入的突發流量特徵值及先前網路行為狀態類別，決定在混合隱藏式馬可夫模型中，對應各個預先定義的網路行為狀態（正常行為狀態、閒置行為狀態和動作行為狀態）的機率值。狀態估算器 191 利用前向式演算法(Forward algorithm)，亦即將利用混合隱藏式馬可夫模型所計算出的各個網路突發流量特徵機率值加總，以計算目前網路的行為狀態在各個預先定義的網路行為狀態的機率值。

狀態對應器 193 從狀態估算器 191 輸入的各個網路行為狀態的機率值，決定目前網路狀態所屬的網路行為狀態類別，且判斷其是否為需警告的網路行為狀態類別，並暫時儲存此網路行為狀態類別。狀態對應器 193 當目前網路的行為狀態所屬的預先定義網路行為狀態為閒置行為狀態

或動作行為狀態則產生警告。

先前狀態暫存器 195 暫存由狀態對應器 193 所產生的網路行為狀態類別，以提供狀態估算器 191 計算下一筆流量在各個網路行為狀態的機率值。

警告資料庫 180 儲存狀態對應器 193 產生的警告訊息，以供後續使用。

第 2 圖顯示依據本發明實施例之殭屍網路偵測方法的流程圖。

步驟 S201 為訓練階段，建立被偵測之網路的混合隱藏式馬可夫模型。步驟 S205 為檢測階段，依據已建立的混合隱藏式馬可夫模型，判斷目前網路之行為狀態類別。

上述訓練階段及檢測階段的詳細步驟如第 3 圖及第 4 圖所示。

第 3 圖顯示第 2 圖之訓練階段的流程圖。

步驟 S301 中，從網路收集封包，並篩選出網際網路中繼聊天(Internet Relay Chat, IRC)封包，擷取並輸出該 IRC 封包的欄位值。

步驟 S303 中，計算突發流量特徵值。在此，突發流量特徵值有二：其一為每秒鐘封包大小的平均值，另一則是每秒鐘封包間隔時間的平均值。

步驟 S305 中，依據該突發流量特徵值，計算各個預先定義的狀態間轉換機率，以產生轉換機率參數。利用條件機率配合統計的計次法則(Counting rule)，依序計算每一筆訓練資料(Instance)所屬的行為狀態類別在整個訓練資料集(Training set)中所佔有的比率，該比率便是該筆資料的轉換機率。

步驟 S307 中，依據該突發流量特徵值，計算該流量突發特徵值符合各個預先定義狀態的可能機率，以產生該輸出機率參數。利用條件機率配合統計的計次法則，計算每一個訓練資料中萃取出的特徵向量值在行為狀態中的機率。

步驟 S309 中，依據該轉換機率參數及輸出機率參數，產生混合隱藏式馬可夫模型之機率時序模型。

第 4 圖顯示第 2 圖中檢測階段的流程圖。

步驟 S401 中，從網路收集封包，並篩選出網際網路中繼聊天(Internet Relay Chat, IRC)封包，擷取並輸出該 IRC 封包的欄位值。

步驟 S402 中，計算突發流量特徵值。在此，突發流量特徵值有二：其一為每秒鐘封包大小的平均值，另一則是每秒鐘封包間隔時間的平均值。

當從一偵測對象網路接收到 IRC 封包，並據以產生突發流量特徵值之後，在步驟 S403 中，依據突發流量特徵值及先前網路行為狀態類別，判斷並儲存目前的網路狀態。亦即，依據突發流量特徵值及先前網路行為狀態類別，決定在混合隱藏式馬可夫模型中，對應各個預先定義的網路行為狀態（正常行為狀態、閒置行為狀態和動作行為狀態）的機率值。

步驟 S404 中，判斷目前的網路狀態是否為閒置行為狀態，若是，則該方法執行步驟 S406，否則，該方法執行步驟 S405。

在步驟 S405 中，判斷目前的網路狀態是否為動作行為狀態，若是，則該方法執行步驟 S406，否則，該方法結束。

在步驟 S406 中，發出並儲存警告訊息。

如上述，本系統設立閒置行為狀態，可以用於偵測早期的殭屍網路流量，即偵測出尚在等待駭客或攻擊者命令的殭屍網路，可於殭屍電腦(Bots)發動攻擊前便可以偵測出來，並提醒管理人員進行處理，以減少因為殭屍網路產生攻擊時的修復成本。

雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

第 1 圖顯示依據本發明實施例之僵屍網路偵測系統之方塊圖。

第 2 圖顯示依據本發明實施例之殭屍網路偵測方法的流程圖。

第 3 圖顯示第 2 圖之訓練階段的流程圖。

第 4 圖顯示第 2 圖中檢測階段的流程圖。

【主要元件符號說明】

僵屍網路偵測系統 100

IRC 網路封包收集器 110

突發流量特徵萃取器 130

模型參數估算器 150

轉換機率參數估算器 151

輸出機率參數估算器 153

模型產生器 170

可疑狀態偵測器 190

狀態估算器 191

狀態對應器 193

先前狀態暫存器 195

警告資料庫 180

七、申請專利範圍：

1.一種僵屍網路偵測系統，其包括：

一突發流量特徵萃取器，接收一偵測對象網路中一網際網路中繼聊天（IRC）封包的欄位值，並據以計算一突發流量特徵值；

一模型參數估算器，依據該突發流量特徵值，決定混合隱藏式馬可夫模型（Hybrid Hidden Markov Model, HHMM）所需之機率參數值，其中該機率參數值包括一轉換機率參數值及一輸出機率參數值，其中該模型參數估算器包括：

一轉換機率參數估算器，其依據該突發流量特徵值，計算各個預先定義的狀態間轉換機率，以產生該轉換機率參數值；及

一輸出機率參數估算器，其依據該突發流量特徵值，計算該流量突發特徵值符合各個預先定義狀態的可能機率，以產生該輸出機率參數值；

一模型產生器，依據該機率參數值，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型；及

一可疑狀態偵測器，當接收到一新的IRC封包，並由突發流量特徵萃取器據以產生突發流量特徵值之後，該可疑狀態偵測器將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型中，據以判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生相對的警告訊息。

2.如申請專利範圍第 1 項所述之僵屍網路偵測系統，

更包括一網際網路中繼聊天（IRC）封包收集器，其從該偵測對象網路收集封包，並從收集之該封包中篩選出網際網路中繼聊天(Internet Relay Chat, IRC)封包，擷取該IRC封包的欄位值，並將該IRC封包的欄位值輸出給該突發流量特徵萃取器。

3.如申請專利範圍第1項所述之僵屍網路偵測系統，其中該突發流量特徵值包括：每秒鐘封包大小的平均值、及每秒鐘封包間隔時間的平均值。

4.如申請專利範圍第1項所述之僵屍網路偵測系統，其中該轉換機率參數估算器利用條件機率配合統計的計次法則(Counting rule)，依序計算每一筆訓練資料(Instance)所屬的行為狀態類別在整個訓練資料集(Training set)中所佔有的比率，該比率即為該筆資料的轉換機率參數值。

5.如申請專利範圍第1項所述之僵屍網路偵測系統，其中該輸出機率參數估算器利用條件機率配合統計的計次法則，計算每一個訓練資料中萃取出的特徵向量值在行為狀態中的機率，作為該輸出機率參數值。

6.如申請專利範圍第1項所述之僵屍網路偵測系統，其中該預先定義的網路行為狀態類別包括正常行為狀態(Normal state)、閒置行為狀態(Idle state)和動作行為狀態(Active state)，其中該閒置行為狀態及該動作行為狀態屬於該可疑流量狀態。

7.如申請專利範圍第1項所述之僵屍網路偵測系統，該可疑狀態偵測器包括：

一狀態估算器，依據該突發流量特徵值及先前網路行為狀態類別，決定在混合隱藏式馬可夫模型中，對應各個

預先定義的網路行為狀態的機率值；

一狀態對應器，依據各個網路行為狀態的機率值，決定目前網路狀態所屬的網路行為狀態類別，且判斷其是否為需警告的網路行為狀態類別；及

一先前狀態暫存器，暫存由該狀態對應器所產生的網路行為狀態類別，以提供該狀態估算器計算下一筆流量在各個網路行為狀態的機率值。

8.如申請專利範圍第7項所述之僵屍網路偵測系統，該狀態估算器將利用混合隱藏式馬可夫模型所計算出的各個網路突發流量特徵機率值加總，以計算目前網路的行為狀態在各個預先定義的網路行為狀態的機率值。

9.如申請專利範圍第1項所述之僵屍網路偵測系統，更包括一警告資料庫，其儲存該警告訊息，以供後續使用。

10.一種殭屍網路偵測方法，其包括：

接收一偵測對象網路中一網際網路中繼聊天（IRC）封包的欄位值，並據以計算一突發流量特徵值；

依據該突發流量特徵值，決定混合隱藏式馬可夫模型（Hybrid Hidden Markov Model, HHMM）所需之機率參數值，其中該機率參數值包括一轉換機率參數值及一輸出機率參數值，該步驟包括：依據該突發流量特徵值，計算各個預先定義的狀態間轉換機率，以產生該轉換機率參數值；及依據該突發流量特徵值，計算該流量突發特徵值符合各個預先定義狀態的可能機率，以產生該輸出機率參數值；

依據該機率參數值，並配合預先定義的網路行為狀態類別，建立混合隱藏式馬可夫模型之機率時序模型；及

當接收到一新的IRC封包，並由突發流量特徵萃取器據以產生突發流量特徵值之後，該可疑狀態偵測器將該突發流量特徵值輸入該混合隱藏式馬可夫模型之機率時序模型中，據以判斷該偵測對象網路的中繼聊天流量狀態是否為可疑流量狀態，若是，則產生相對的警告訊息。

11.如申請專利範圍第 10 項所述之殭屍網路偵測方法，更從該偵測對象網路收集封包，並從收集之該封包中篩選出網際網路中繼聊天(Internet Relay Chat, IRC)封包，擷取該IRC封包的欄位值。

12.如申請專利範圍第 10 項所述之殭屍網路偵測方法，其中該突發流量特徵值包括：每秒鐘封包大小的平均值、及每秒鐘封包間隔時間的平均值。

13.如申請專利範圍第 10 項所述之殭屍網路偵測方法，利用條件機率配合統計的計次法則(Counting rule)，依序計算每一筆訓練資料(Instance)所屬的行為狀態類別在整個訓練資料集(Training set)中所佔有的比率，該比率即為該筆資料的轉換機率。

14.如申請專利範圍第 10 項所述之殭屍網路偵測方法，利用條件機率配合統計的計次法則，計算每一個訓練資料中萃取出的特徵向量值在行為狀態中的機率，作為該輸出機率參數值。

15.如申請專利範圍第 10 項所述之殭屍網路偵測方法，其中該預先定義的網路行為狀態類別包括正常行為狀態(Normal state)、閒置行為狀態(Idle state)和動作行為狀態(Active state)，其中該閒置行為狀態及該動作行為狀態屬於該可疑流量狀態。

16.如申請專利範圍第 10 項所述之殭屍網路偵測方法，更包括：

依據該突發流量特徵值及先前網路行為狀態類別，決定在混合隱藏式馬可夫模型中，對應各個預先定義的網路行為狀態的機率值；

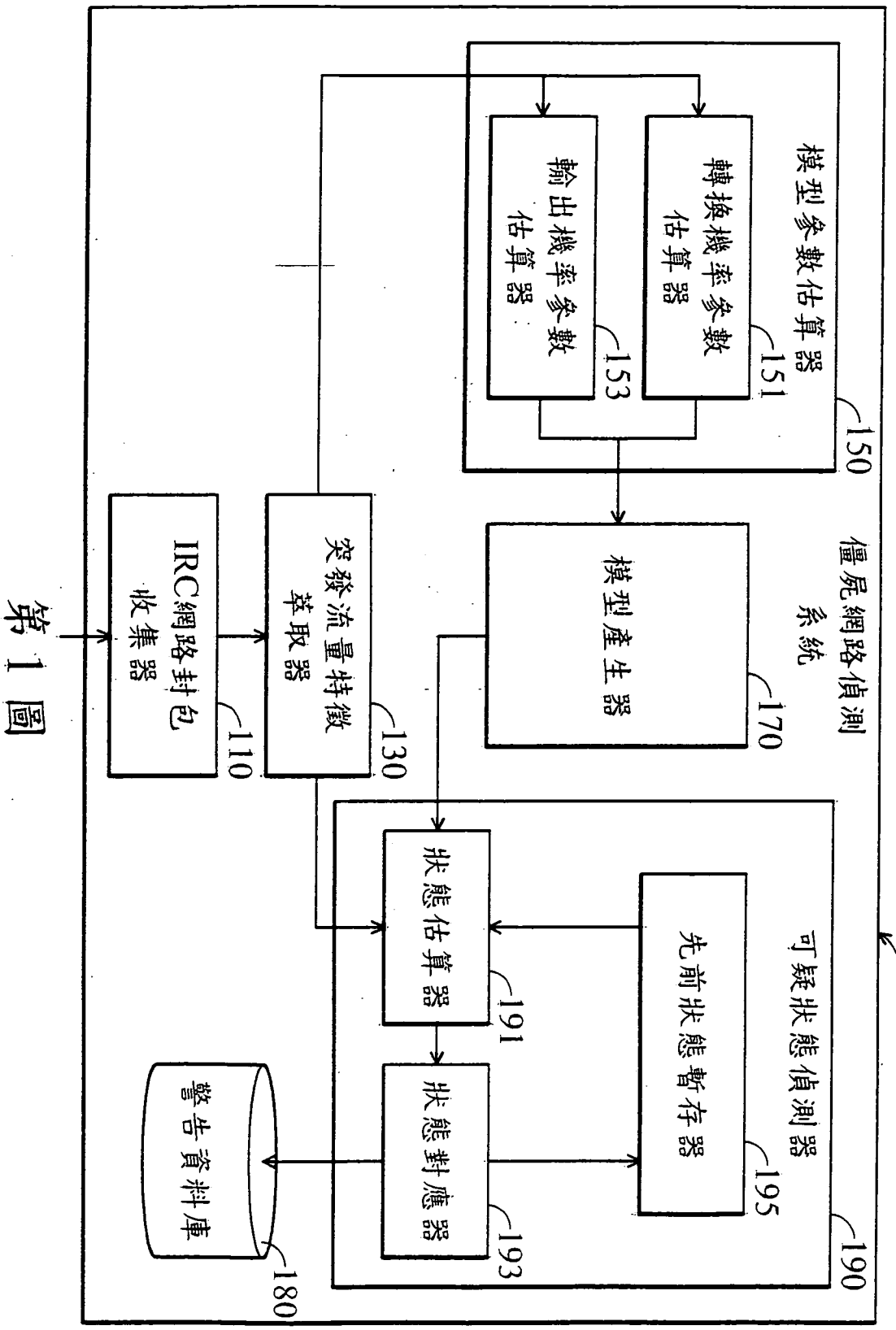
依據各個網路行為狀態的機率值，決定目前網路狀態所屬的網路行為狀態類別，且判斷其是否為需警告的網路行為狀態類別；及

暫存由該狀態對應器所產生的網路行為狀態類別，以提供計算下一筆流量在各個網路行為狀態的機率值之用。

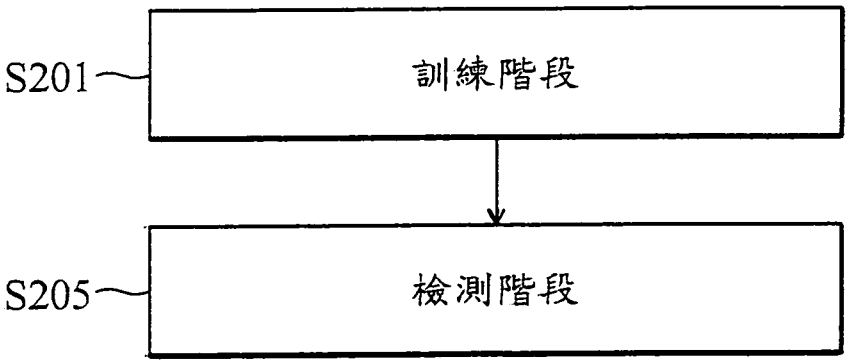
17.如申請專利範圍第 16 項所述之殭屍網路偵測方法，將利用混合隱藏式馬可夫模型所計算出的各個網路突發流量特徵機率值加總，以計算目前網路的行為狀態在各個預先定義的網路行為狀態的機率值。

18.如申請專利範圍第 10 項所述之殭屍網路偵測方法，更儲存該警告訊息，以供後續使用。

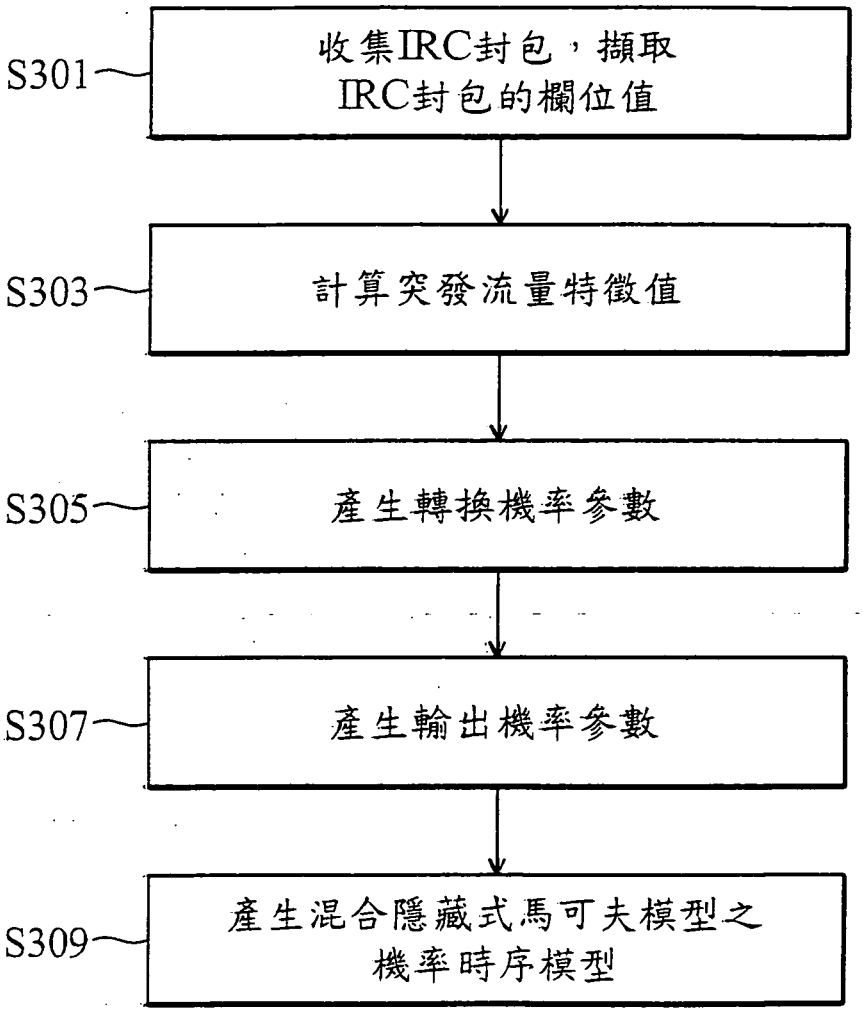
I405434


100
殭屍網路偵測系統
模型參數估算器
150
轉換機率參數估算器
151
輸出機率參數估算器
153
模型產生器
170
突發流量特徵萃取器
130
IRC網路封包收集器
110
可疑狀態偵測器
190
先前狀態暫存器
195
狀態估算器
191
狀態對應器
193
警告資料庫
180

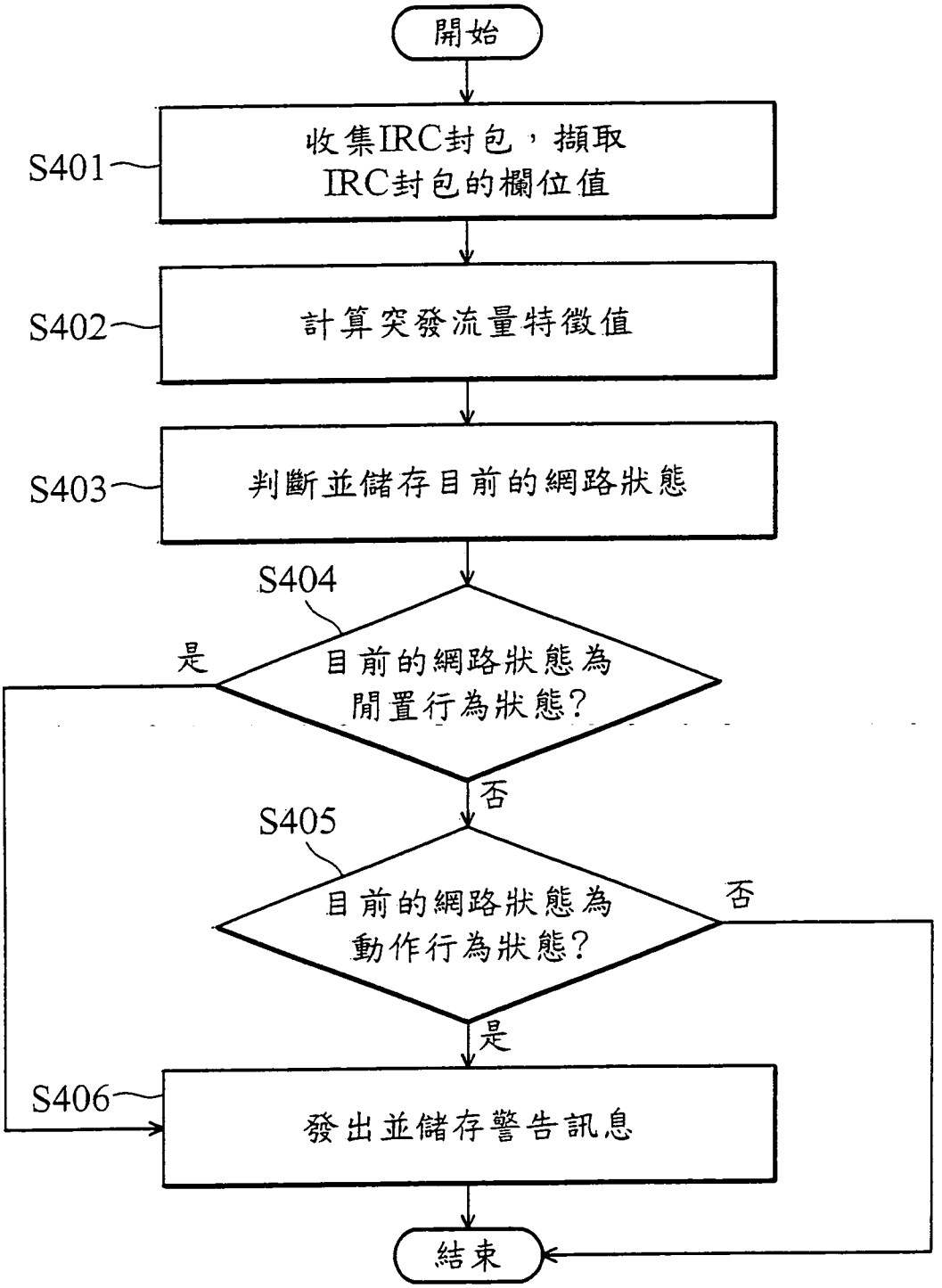
第 1 圖



第 2 圖


S301
收集IRC封包，擷取
IRC封包的欄位值
S303
計算突發流量特徵值
S305
產生轉換機率參數
S307
產生輸出機率參數
S309
產生混合隱藏式馬可夫模型之
機率時序模型

第 3 圖


開始
S401
收集IRC封包，擷取
IRC封包的欄位值
S402
計算突發流量特徵值
S403
判斷並儲存目前的網路狀態
S404
是
目前的網路狀態為
閒置行為狀態?
否
S405
目前的網路狀態為
動作行為狀態?
否
是
S406
發出並儲存警告訊息
結束

第 4 圖