(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201216106 A1
(43)公開日： 中華民國 101 (2012) 年 04 月 16 日

(21)申請案號：099134925 (22)申請日： 中華民國 99 (2010) 年 10 月 13 日
(51)Int. Cl.： *G06F21/00 (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) ；葉治宏 YEH, JEROME (TW) ；余威逸 YU, WEI YI (TW)
(74)代理人：詹銘文；葉璟宗
申請實體審查：有 申請專利範圍項數：9 項 圖式數：8 共 26 頁

(54)名稱

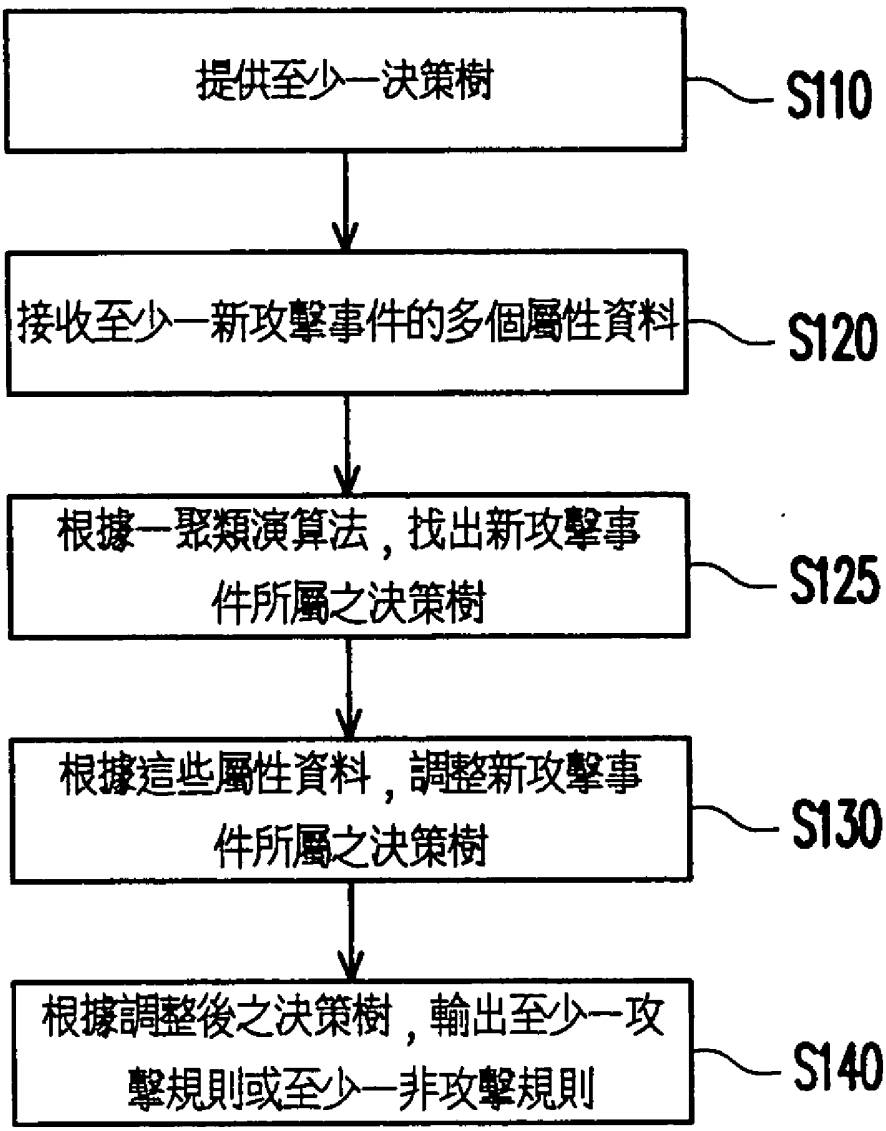
入侵偵測系統及其分類規則的產生方法

INTRUSION DETECTING SYSTEM AND METHOD TO ESTABLISH CLASSIFYING RULES THEREOF

(57)摘要

一種入侵偵測系統之分類規則的產生方法，其包括下列步驟。首先，提供至少一決策樹。決策樹的內部節點分別表示一屬性判斷條件，而決策樹的葉節點分別表示一攻擊事件或一非攻擊事件。接著，接收至少一新攻擊事件的多個屬性資料。然後，根據這些屬性資料，調整決策樹的樹狀結構。之後，根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則。此外，本發明亦提出一種入侵偵測系統。

S110~S140：步驟


提供至少一決策樹
S110
接收至少一新攻擊事件的多個屬性資料
S120
根據一聚類演算法，找出新攻擊事件所屬之決策樹
S125
根據這些屬性資料，調整新攻擊事件所屬之決策樹
S130
根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則
S140

六、發明說明：

【發明所屬之技術領域】

本發明係與一種網路事件的處理方法與系統有關，且特別係與一種偵測網路入侵事件的方法與系統有關。

【先前技術】

在資訊時代可以透過網際網路來連結全球各地之電腦，現今不論是企業或是個人均已普遍利用網際網路來傳送或存取資料。但是，隨著網路的普及化，網路攻擊事件卻層出不窮，網路安全愈來愈受到重視。在大家所熟知的網路安全機制中，入侵偵測系統（Intrusion Detection System，IDS）扮演相當重要的角色。入侵偵測系統主要是用來監視網路或系統所發生的事件，並根據預先建立好的規則來將事件分類為攻擊與非攻擊事件。當發現攻擊事件時，系統除發送警訊通報給網管人員，還可即採取必要的處置措施，例如阻斷來源IP。因此，一個優良的入侵偵測系統將可以有效地增加網路系統的安全性。

一般而言，傳統的入侵偵測系統會透過批次離線學習的方式來產生分類規則。然而，在遇到新型態的攻擊時，往往需要重新批次離線學習。此時，入侵偵測系統需要離線而停止偵測的工作，且必須將新型態的攻擊事件加入原有的樣本事件中，再對所有的事件進行重新學習，並重新產生整個規則資料庫。

【發明內容】

本發明提供一種入侵偵測系統及其分類規則的產生方法，能夠即時調整偵測入侵事件的分類規則。

本發明提出一種入侵偵測系統之分類規則的產生方法，其包括下列步驟。首先，提供至少一決策樹（decision tree）。決策樹的內部節點（internal node）分別表示一屬性判斷條件（attribute judgment condition），而決策樹的葉節點（leaf node）分別表示一攻擊事件（attack event）或一非攻擊事件（non-attack event）。接著，接收至少一新攻擊事件的多個屬性資料。然後，根據這些屬性資料，調整決策樹的樹狀結構。之後，根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則。

在本發明之一實施例中，調整決策樹的樹狀結構的步驟，包括根據一遞增樹推導（incremental tree induction）方式，調整決策樹的樹狀結構。

在本發明之一實施例中，在調整決策樹的樹狀結構的步驟之前，入侵偵測系統之分類規則的產生方法更包括正規化這些屬性資料成多個數值資料，其中這些數值資料大於等於0且小於等於1。

在本發明之一實施例中，其中在調整決策樹的樹狀結構的步驟之前，入侵偵測系統之分類規則的產生方法更包括根據一聚類演算法，找到新攻擊事件所屬之決策樹，以調整新攻擊事件所屬之決策樹。

在本發明之一實施例中，其中在調整決策樹的樹狀結

構的步驟之前，入侵偵測系統之分類規則的產生方法，更包括根據一顯著屬性清單，從這些屬性資料中挑出至少一顯著屬性資料，以根據這些顯著屬性資料執行聚類演算法。

在本發明之一實施例中，提供決策樹的步驟包括批次及線上即時學習多個訓練事件來建立決策樹。

本發明再提出一種入侵偵測系統，包括一決策樹模組、一前處理模組、一聚類模組、一調整模組、一規則輸出模組以及一攻擊規則資料庫。決策樹模組用以儲存至少一決策樹。決策樹的內部節點分別表示一屬性判斷條件，而決策樹的葉節點分別表示一攻擊事件或一非攻擊事件。前處理模組係用以接收至少一新攻擊事件的多個屬性資料。聚類模組係用以將相似屬性資料聚集在同一群。調整模組係用以根據這些屬性資料，調整決策樹的樹狀結構。規則輸出模組係用以根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則。攻擊規則資料庫則係用以儲存攻擊規則或非攻擊規則。

在本發明之一實施例中，入侵偵測系統更包括一聚類模組。聚類模組會根據一聚類演算法，找到新攻擊事件所屬之決策樹，以讓調整模組調整新攻擊事件所屬之決策樹。

在本發明之一實施例中，入侵偵測系統更包括一顯著屬性清單模組，用以儲存一顯著屬性清單。聚類模組根據顯著屬性清單，從這些屬性資料中挑出至少一顯著屬性資料，以根據這些顯著屬性資料執行聚類演算法。

在本發明之一實施例中，入侵偵測系統更包括一警示

訊息產生模組與一警示訊息資料庫。警示訊息產生模組係用以在受到攻擊時，根據攻擊規則資料庫發出一警示訊息。警示訊息資料庫用以儲存警示訊息。

基於上述，本發明能夠根據新攻擊事件調整決策樹的樹狀結構，而對應輸出攻擊或非攻擊規則。因此，不需對所有樣本重新學習，即可即時更新入侵偵測的規則，使得入侵偵測的能力得以提升。

為讓本發明之上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【實施方式】

圖 1 為本發明一實施例之入侵偵測系統的示意圖。請參考圖 1，入侵偵測系統 100 包括一前處理模組 110、一聚類模組 160、一決策樹模組 120、一調整模組 130、一規則輸出模組 140 以及一攻擊規則資料庫 150。前處理模組 110 係用以接收至少一新攻擊事件的多個屬性資料。這些屬性資料包括連線停留時間、TCP/UDP 服務、封包大小等網路資訊。

圖 2A 為圖 1 之決策樹模組所儲存的決策樹的示意圖。請配合參考圖 2A，決策樹模組 120 用以儲存至少一決策樹 T1。決策樹 T1 的內部節點 I1~I3 分別表示一屬性判斷條件，而決策樹 T1 的葉節點 L1~L4 分別表示一攻擊事件或一非攻擊事件。舉例來說，內部節點 I1 代表判斷來源送出的資料是否小於 326.50 bytes，葉節點 L1 代表非攻擊

事件（以 0 表示），而葉節點 L3 代表 warezclient 攻擊事件（以 1 表示）。聚類模組 160 用以將相似屬性資料聚集在同一群，並根據一聚類演算法，從決策樹模組 120 中找到新攻擊事件所屬之決策樹 T1。

圖 2B 為圖 2A 之決策樹在調整後的示意圖。請參考圖 2A 與圖 2B，調整模組 130 用以根據這些屬性資料，調整新攻擊事件所屬之決策樹 T1 的樹狀結構（以決策樹 T2 表示）。如圖 2B 所示，相較於決策樹 T1，決策樹 T2 增加了內部節點 I4、I5 以及葉節點 L5、L6。規則輸出模組 140 用以根據調整後之決策樹 T2，輸出至少一攻擊規則或至少一非攻擊規則。舉其中一攻擊規則為例來說，當事件符合（dst_host_srv_count > 254.50） and （service = private）時，即代表 snmpguess 攻擊事件（以 1 表示）。攻擊規則資料庫 150 用以儲存攻擊規則或非攻擊規則。

圖 3 為圖 1 之入侵偵測系統之分類規則的產生方法的流程圖。請參考圖 1 與圖 3，入侵偵測系統 100 的動作可大致歸納出以下的流程。首先進行步驟 S110，提供至少一決策樹 T1（如圖 2A）。接著進行步驟 S120，接收至少一新攻擊事件的多個屬性資料。再來進行步驟 S125，根據一聚類演算法，找到新攻擊事件所屬之決策樹 T1。然後進行步驟 S130，根據這些屬性資料，調整新攻擊事件所屬之決策樹 T1 的樹狀結構（以圖 2B 的決策樹 T2 表示）。之後進行步驟 S140，根據調整後之決策樹 T2，輸出至少一攻擊規則或至少一非攻擊規則。亦即，根據決策樹 T2 的分

支 T、F、內部節點 I1~I5 與葉節點 L1~L6 所構成的路徑來產生規則。

值得一提的是，若是發現有新型態的攻擊時，只要根據新型態的攻擊來調整決策樹，即可線上即時地更新分類規則，而不需離線重新對所有訓練樣本進行學習。

圖 4 為本發明一實施例之入侵偵測系統的示意圖，圖 5 為圖 4 之入侵偵測系統之分類規則的產生方法的流程圖。以下將配合圖 4 的入侵偵測系統 200 與圖 5 的流程來說明，且相似元件與步驟將不再贅述。

請先參考圖 4，相較於入侵偵測系統 100，入侵偵測系統 200 更可包括一資料型態錯誤報告模組 260、一聚類模組 270、一顯著屬性清單模組 280、一警示訊息產生模組 290 以及一警示訊息資料庫 295。資料型態錯誤報告模組 260 用以在前處理模組 210 接收到錯誤型態的屬性資料時，產生資料型態錯誤報告。聚類模組 270 用以根據一聚類演算法，找到新攻擊事件所屬之決策樹。在本實施例中，聚類演算法例如為 K-means 或 SOM 聚類方法。顯著屬性清單模組 280 用以儲存一顯著屬性清單。在本實施例中，顯著屬性清單例如可根據 KDD'99 資料集的特徵來定義出一些顯著屬性。警示訊息產生模組 290 用以在受到攻擊時，根據攻擊規則資料庫 250 發出一警示訊息。用以儲存警示訊息。

請參考圖 4 與圖 5，首先進行步驟 S210，提供至少一決策樹（詳細步驟將配合圖 6 進行說明）。接著進行步驟

S220，前處理模組210接收至少一新攻擊事件的多個屬性資料。然後進行步驟S230，藉由前處理模組210正規化這些屬性資料成多個數值資料。舉例來說，前處理模組210可將符號型資料經由預先定義好的轉換表（mapping table）轉換成數值資料，並將數值資料正規化成介於0和1之間的數值。在本實施例中，若是前處理模組210無法將輸入的資料轉換成數值性資料或格式錯誤時，還可藉由資料型態錯誤報告模組260發出錯誤報給系統管理者。

接著進行步驟S240，聚類模組270根據顯著屬性清單，從這些屬性資料中挑出至少一顯著屬性資料，以根據這些顯著屬性資料執行聚類演算法來分群。亦即，相似或相同服務（如HTTP服務）的攻擊事件或正常事件聚集在同一群。在本實施例中，顯著屬性清單可由人工定義已知攻擊之顯著屬性。在顯著屬性清單中，0代表不顯著屬性，聚類模組270忽略不顯著屬性值不予以處理；1代表顯著屬性，聚類模組270會處理顯著屬性，並計算各事件屬性之距離，以將距離相近（相似）事件聚集在同一群。

圖7為示意根據顯著屬性清單聚類的決策樹。如圖7所示，決策樹T3包括一內部節點I6與二葉節點L7、L8。由於屬性hot足以區分攻擊事件（back）和正常事件（normal），所以由人工在顯著屬性清單定義hot屬性為1，而其他屬性設為0。在此設定下，聚類模組270只對hot屬性進行計算，而忽略其他屬性。如此一來，事件便可聚集成兩群，一群為正常事件，另一群為攻擊事件。

之後進行步驟 S250，聚類模組 270 根據一聚類演算法，找到新攻擊事件所屬之決策樹。接著進行步驟 S260，調整模組 230 根據一遞增樹推導方式，調整新攻擊事件所屬之決策樹的樹狀結構。在另一未繪示的實施例中，亦可利用高度平衡二元搜尋樹（AVL-tree）的概念來調整決策樹的樹狀結構。然後進行步驟 S270，規則輸出模組 240 根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則至攻擊規則資料庫 250。

圖 6 為圖 5 之提供決策樹步驟的詳細流程圖。請參考圖 6，在本實施例中，決策樹可由批次學習多個訓練事件來建立，其中訓練事件可包括多個攻擊事件與多個正常事件。詳細來說，首先進行步驟 S310，前處理模組 210 接收各種型態攻擊及正常事件的屬性資料的輸入。接著進行步驟 S320，並藉由前處理模組 210 正規化這些屬性資料成多個數值資料。之後進行步驟 S330，聚類模組 270 根據聚類演算法與顯著屬性清單，將各型態攻擊及正常事件歸屬於不同群組。詳細來說，可進行以下兩種處理。第一，聚類模組 270 接收前處理模組 210 所輸出之正規化數值資料。然後，依據顯著屬性清單模組 280 的顯著屬性清單來計算各屬性值之距離（如歐基里德距離）。之後，依各屬性值之距離來計算其相似度，並輸出每一屬性值之分群。第二，依不同服務來分群，並輸出每一屬性值之分群。

然後進行步驟 S340，調整模組 230 依據不同群組之攻擊事件及正常事件的屬性資料，產生各群組分別對應的決

策樹。再來進行步驟S350，規則輸出模組240根據不同群組所對應的決策樹，輸出至少一攻擊規則或至少一非攻擊規則至攻擊規則資料庫250。

圖8為圖4之入侵偵測系統於檢測階段的流程圖。請參考圖8，在前述批次學習（步驟S310~S350）與漸進式學習的階段（步驟S210~S270）之後，即可利用入侵偵測系統來對網路上的事件進行檢測。首先進行步驟S410，前處理模組210接收至少一事件。接著進行步驟S420，輸入事件的屬性資料至前處理模組210。然後進行步驟S430，前處理模組210正規化這些屬性資料成多個數值資料。之後進行步驟S440，聚類模組270根據聚類演算法與顯著屬性清單，將事件歸屬到對應的群組。再來進行步驟S450，警示訊息產生模組290根據事件所對應的群組，找出對應之決策樹。接著進行步驟S460，警示訊息產生模組290由該決策樹所對應的規則判斷事件是否為攻擊事件。當事件被警示訊息產生模組290判斷為攻擊事件時，進行步驟S470，發出並儲存警示訊息至警示訊息資料庫295。

綜上所述，本發明先應用聚類方法將相似事件聚集在同一群後，再根據新攻擊事件來更新決策樹。藉此，即使出現權限提升攻擊（user to root）及遠端登入攻擊（remote to local）等較嚴重的攻擊，皆不需對整個系統重新學習。

雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，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，故本

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】

圖 1 為本發明一實施例之入侵偵測系統的示意圖。

圖 2A 為圖 1 之決策樹模組所儲存的決策樹的示意圖。

圖 2B 為圖 2A 之決策樹在調整後的示意圖。

圖 3 為圖 1 之入侵偵測系統之分類規則的產生方法的流程圖。

圖 4 為本發明一實施例之入侵偵測系統的示意圖。

圖 5 為圖 4 之入侵偵測系統之分類規則的產生方法的流程圖。

圖 6 為圖 5 之提供決策樹步驟的詳細流程圖。

圖 7 為示意根據顯著屬性清單聚類的決策樹。

圖 8 為圖 4 之入侵偵測系統於檢測階段的流程圖。

【主要元件符號說明】

100、200：入侵偵測系統

110、210：前處理模組

120、220：決策樹模組

130、230：調整模組

140、240：規則輸出模組

150、250：攻擊規則資料庫

260：資料型態錯誤報告模組

160、270：聚類模組

280：顯著屬性清單模組

290：警示訊息產生模組

295：警示訊息資料庫

I1~I5：內部節點

L1~L6：葉節點

T1 T2、T3：決策樹

T、F：分支

S110~S140、S210~S270、S310~S350、S410~S470：步驟

201216106

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： 099134925

※ 申請日： 99.10.13 ※IPC 分類： G06F 21/00 (2006.01)

一、發明名稱：

入侵偵測系統及其分類規則的產生方法

INTRUSION DETECTING SYSTEM AND METHOD TO ESTABLISH CLASSIFYING RULES THEREOF

二、中文發明摘要：

一種入侵偵測系統之分類規則的產生方法，其包括下列步驟。首先，提供至少一決策樹。決策樹的內部節點分別表示一屬性判斷條件，而決策樹的葉節點分別表示一攻擊事件或一非攻擊事件。接著，接收至少一新攻擊事件的多個屬性資料。然後，根據這些屬性資料，調整決策樹的樹狀結構。之後，根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則。此外，本發明亦提出一種入侵偵測系統。

三、英文發明摘要：

A method to establish classifying rules of an intrusion detecting system is provided with the following steps. First, at least one decision tree is provided. Each of the internal nodes of the decision tree is respectively represented an

attribute judgment condition, and each of the leaf nodes is respectively represented an attack event or non-attack event. Next, a plurality of attribute data of at least one new attack event is received. Then, structure of the decision tree is adjusted according to the attribute data. Afterwards, at least one attack rule or at least one non-attack rule is outputted according to the decision tree adjusted. Further, the intrusion detection system is also provided.

四、指定代表圖：

（一）本案之指定代表圖：圖 3

（二）本代表圖之元件符號簡單說明：

S110~S140：步驟

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

七、申請專利範圍：

1. 一種入侵偵測系統之分類規則的產生方法，包括：

提供至少一決策樹，其中該決策樹的內部節點分別表示一屬性判斷條件，而該決策樹的葉節點分別表示一攻擊事件或一非攻擊事件；

接收至少一新攻擊事件的多個屬性資料；

根據一聚類演算法，找到該新攻擊事件所屬之決策樹；

根據該些屬性資料，調整該新攻擊事件所屬之決策樹的樹狀結構；以及

根據調整後之該決策樹，輸出至少一攻擊規則或至少一非攻擊規則。

2. 如申請專利範圍第 1 項所述之入侵偵測系統之分類規則的產生方法，其中調整該決策樹的樹狀結構的步驟，包括：

根據一遞增樹推導方式，調整該決策樹的樹狀結構。

3. 如申請專利範圍第 1 項所述之入侵偵測系統之分類規則的產生方法，其中在調整該決策樹的樹狀結構的步驟之前，更包括：

正規化該些屬性資料成多個數值資料，其中該些數值資料大於等於 0 且小於等於 1。

4. 如申請專利範圍第 1 項所述之入侵偵測系統之分類規則的產生方法，其中在調整該決策樹的樹狀結構的步驟之前，包括：

根據一顯著屬性清單，從該些屬性資料中挑出至少一顯著屬性資料，以根據該些顯著屬性資料執行該聚類演算法。

5. 如申請專利範圍第 1 項所述之入侵偵測系統之分類規則的產生方法，其中提供該決策樹的步驟，包括：

批次學習多個訓練事件來建立該決策樹。

6. 一種入侵偵測系統，包括：

一決策樹模組，用以儲存至少一決策樹，其中該決策樹的內部節點分別表示一屬性判斷條件，而該決策樹的葉節點分別表示一攻擊事件或一非攻擊事件；

一前處理模組，用以接收至少一新攻擊事件的多個屬性資料；

一聚類模組，用以根據一聚類演算法，找到該新攻擊事件所屬之決策樹

一調整模組，用以根據該些屬性資料，調整該新攻擊事件所屬之決策樹的樹狀結構；以及

一規則輸出模組，用以根據調整後之該決策樹，輸出至少一攻擊規則或至少一非攻擊規則；以及

一攻擊規則資料庫，用以儲存該攻擊規則或該非攻擊規則。

7. 如申請專利範圍第 6 項所述之入侵偵測系統，更包括：

一顯著屬性清單模組，用以儲存一顯著屬性清單，以讓該聚類模組根據該顯著屬性清單，從該些屬性資料中挑

出至少一顯著屬性資料，以根據該些顯著屬性資料執行該聚類演算法。

8. 如申請專利範圍第6項所述之入侵偵測系統，其中該前處理模組更用以正規化該些屬性資料成多個數值資料，其中該些數值資料大於等於0且小於等於1。

9. 如申請專利範圍第6項所述之入侵偵測系統，更包括：

一警示訊息產生模組，用以在受到攻擊時，根據該攻擊規則資料庫產生一警示訊息；以及

一警示訊息資料庫，用以儲存該警示訊息。

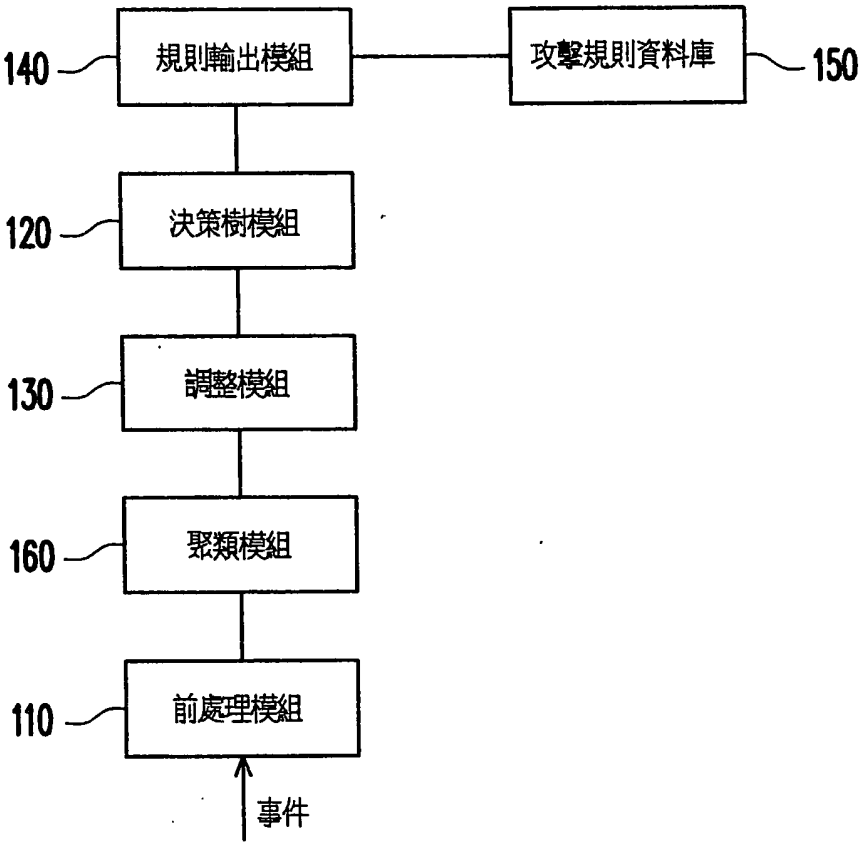

140
規則輸出模組
攻擊規則資料庫
150
120
決策樹模組
130
調整模組
160
聚類模組
110
前處理模組
事件

圖 1

32911TW_M

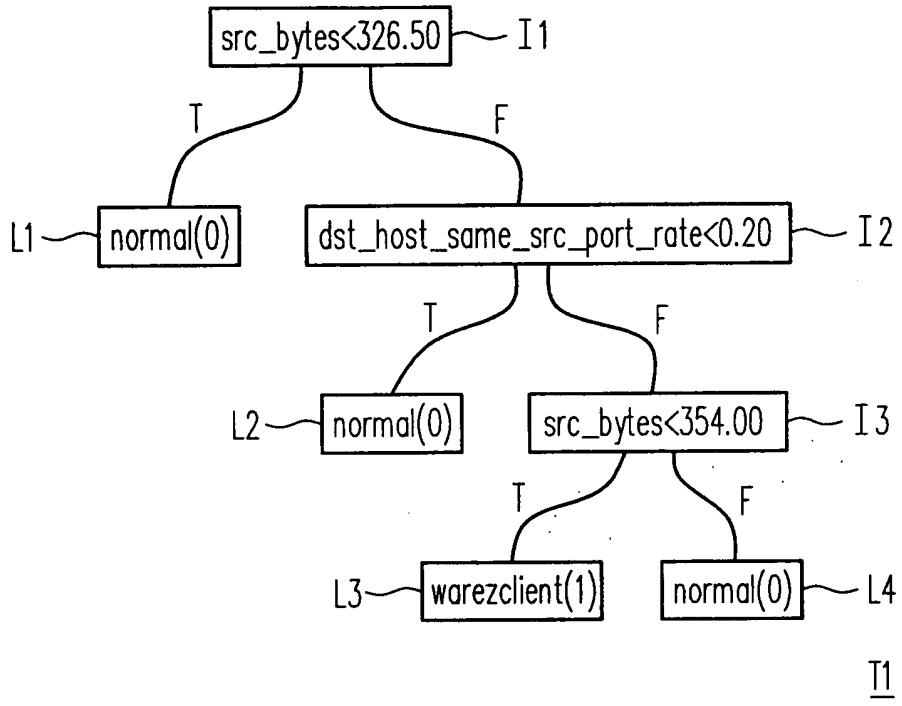


圖 2A

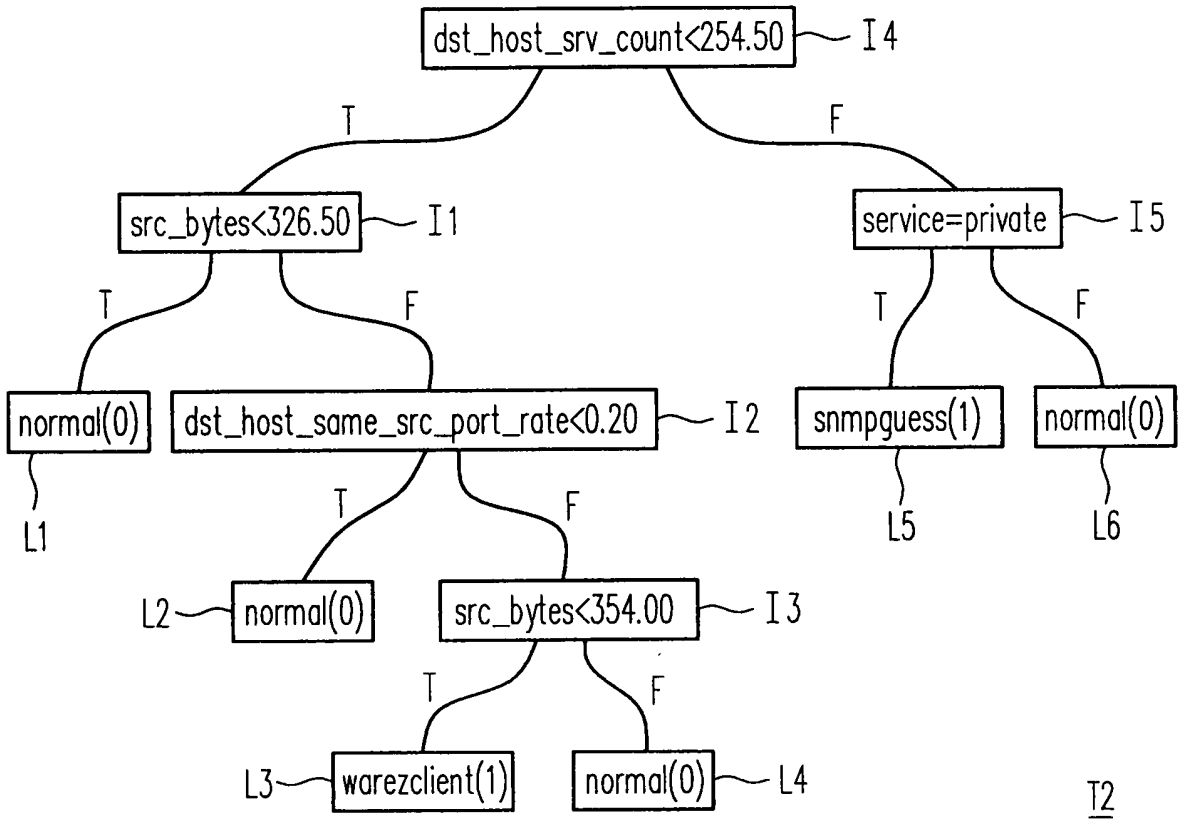


圖 2B

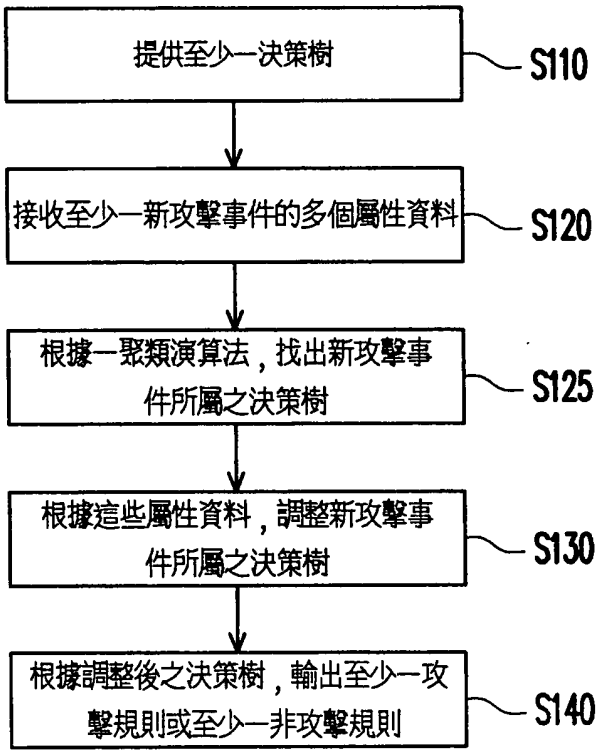

提供至少一決策樹
S110
接收至少一新攻擊事件的多個屬性資料
S120
根據一聚類演算法，找出新攻擊事件所屬之決策樹
S125
根據這些屬性資料，調整新攻擊事件所屬之決策樹
S130
根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則
S140

圖 3

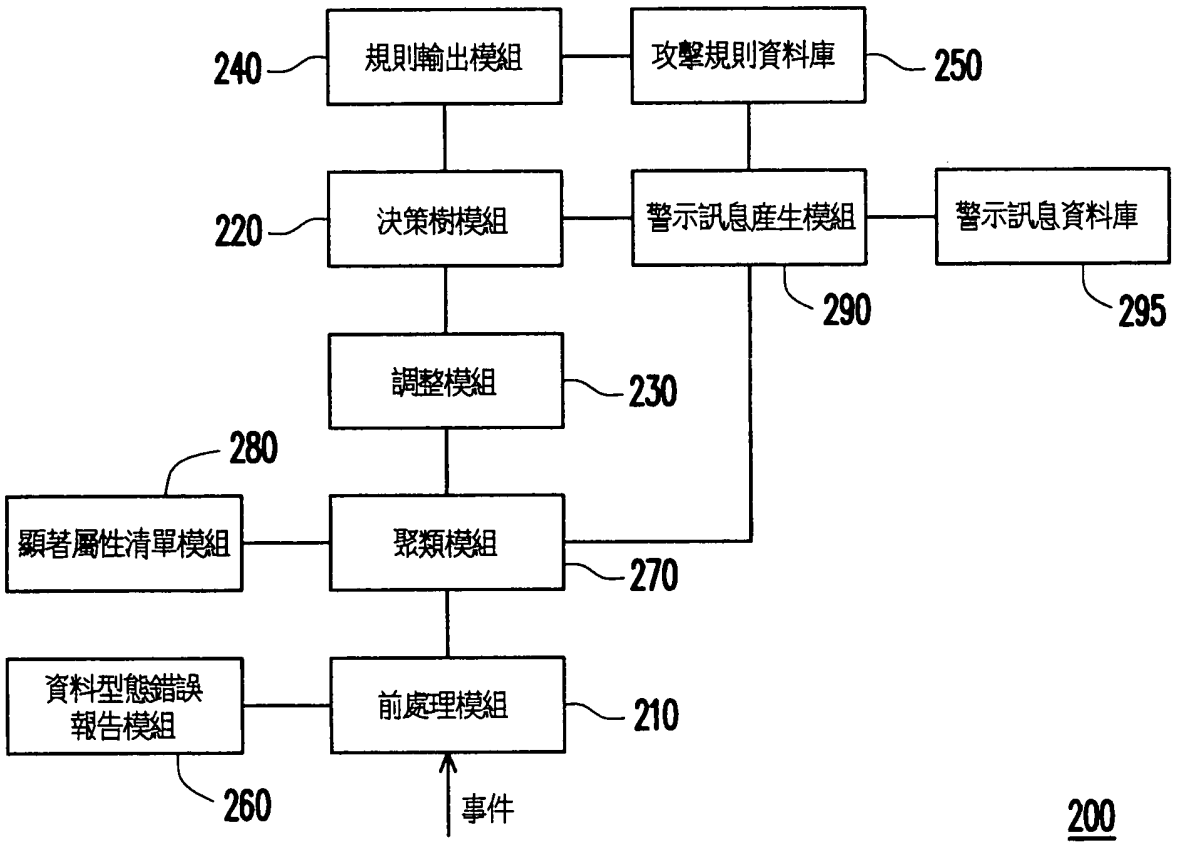

240
規則輸出模組
攻擊規則資料庫
250
220
決策樹模組
警示訊息產生模組
警示訊息資料庫
290
295
調整模組
230
280
顯著屬性清單模組
聚類模組
270
資料型態錯誤
報告模組
前處理模組
210
260
事件
200

圖 4

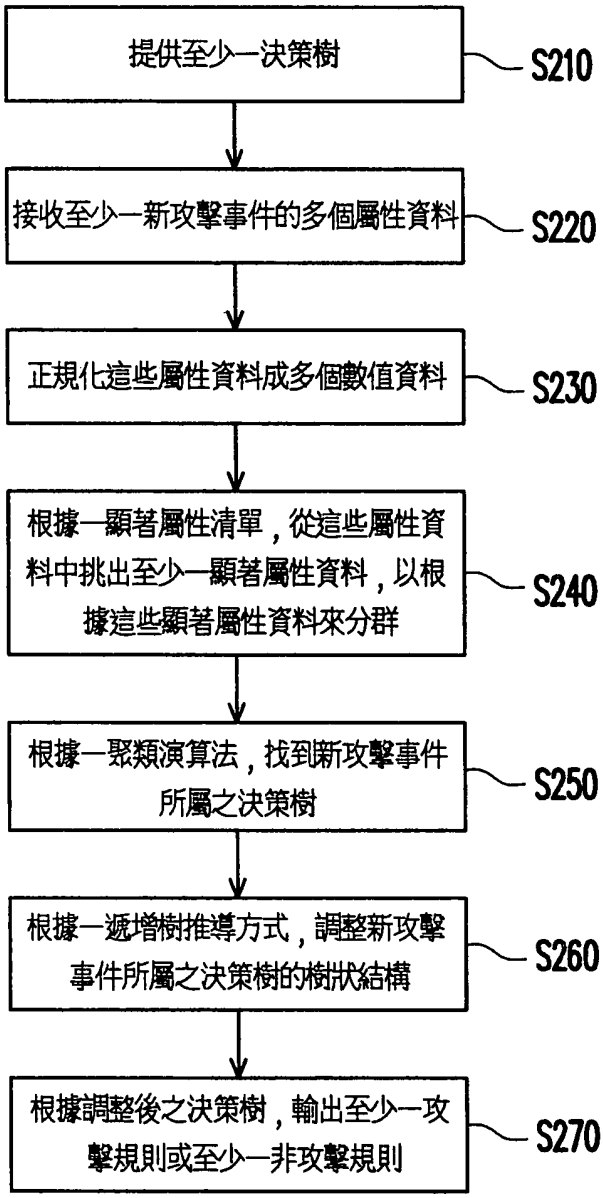

提供至少一決策樹
S210
接收至少一新攻擊事件的多個屬性資料
S220
正規化這些屬性資料成多個數值資料
S230
根據一顯著屬性清單，從這些屬性資料中挑出至少一顯著屬性資料，以根據這些顯著屬性資料來分群
S240
根據一聚類演算法，找到新攻擊事件所屬之決策樹
S250
根據一遞增樹推導方式，調整新攻擊事件所屬之決策樹的樹狀結構
S260
根據調整後之決策樹，輸出至少一攻擊規則或至少一非攻擊規則
S270

圖 5

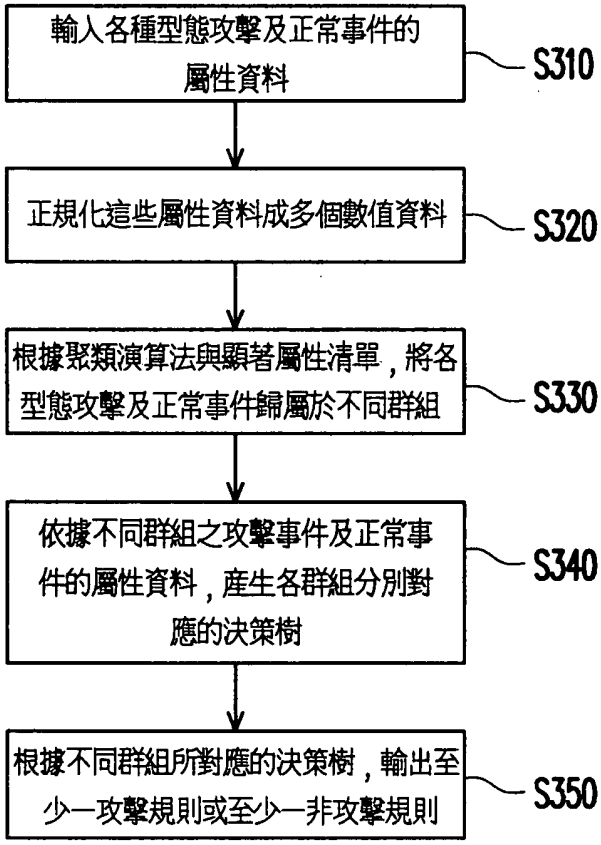

輸入各種型態攻擊及正常事件的屬性資料
S310
正規化這些屬性資料成多個數值資料
S320
根據聚類演算法與顯著屬性清單，將各型態攻擊及正常事件歸屬於不同群組
S330
依據不同群組之攻擊事件及正常事件的屬性資料，產生各群組分別對應的決策樹
S340
根據不同群組所對應的決策樹，輸出至少一攻擊規則或至少一非攻擊規則
S350

圖 6

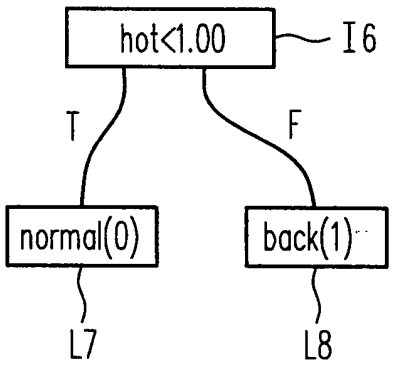


圖 7

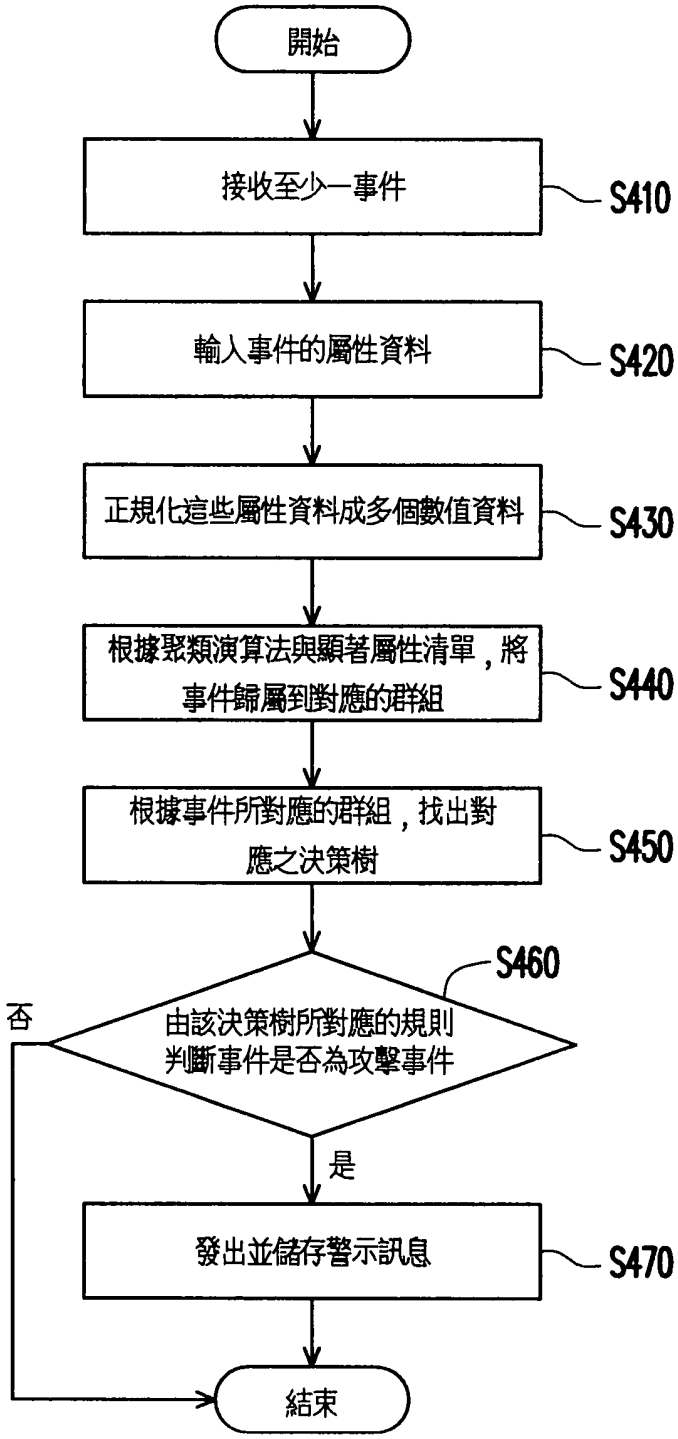

開始
接收至少一事件
S410
輸入事件的屬性資料
S420
正規化這些屬性資料成多個數值資料
S430
根據聚類演算法與顯著屬性清單，將事件歸屬到對應的群組
S440
根據事件所對應的群組，找出對應之決策樹
S450
S460
由該決策樹所對應的規則判斷事件是否為攻擊事件
否
是
發出並儲存警示訊息
S470
結束

圖 8

attribute judgment condition, and each of the leaf nodes is respectively represented an attack event or non-attack event. Next, a plurality of attribute data of at least one new attack event is received. Then, structure of the decision tree is adjusted according to the attribute data. Afterwards, at least one attack rule or at least one non-attack rule is outputted according to the decision tree adjusted. Further, the intrusion detection system is also provided.

四、指定代表圖：

（一）本案之指定代表圖：圖 3

（二）本代表圖之元件符號簡單說明：

S110~S140：步驟

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