【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I893425
【45】公告日： 中華民國 114 (2025) 年 08 月 11 日
【51】Int. Cl.：　*H04L43/062 (2022.01)*　*H04L43/0823(2022.01)*
發明　全 6 頁

【54】名　稱：混合型流量與封包異常偵測系統及方法

【21】申請案號：112130101　【22】申請日： 中華民國 112 (2023) 年 08 月 10 日
【11】公開編號：202508258　【43】公開日期： 中華民國 114 (2025) 年 02 月 16 日

【72】發 明 人： 林盈達 (TW) LIN, YING-DAR；狄　書亞 (ID) SUDYANA, DIDIK；費　亞坦 (ID) YUDHA, FIETYATA；賴佳宏 (TW) LAI, CHIA HUNG
【71】申 請 人： 國立陽明交通大學　NATIONAL YANG MING CHIAO TUNG UNIVERSITY
新竹市大學路 1001 號
【74】代 理 人： 吳冠賜；蘇建太；林志鴻

【56】參考文獻：
US　20220321588A1

審查人員：林宥辰

【57】申請專利範圍

1. 一種混合型流量與封包異常偵測系統，包含：
一封包處理模組(3)，用於判斷進入該混合型流量與封包異常偵測系統(100)的一封包屬於一現存流量或一新流量的一起始封包，該判斷是基於將該封包的一屬性與該現存流量的一屬性進行比對；
一流量追蹤模組(4)；
一基於流量偵測模組(5)；
一基於封包偵測模組(6)；
一灰色區域模組(7)；以及
一控制模組(2)，用於控制該流量追蹤模組(4)、該基於流量偵測模組(5)、該基於封包偵測模組(6)及該灰色區域模組(7)，並執行下列步驟：
針對每一流量，藉由該流量追蹤模組(4)，判斷該流量等待一個新封包到達的一時間量是否超過一第一時間門檻值(T2)，其中該第一時間門檻值(T2)是系統預設的一最大封包等待時間；
當該流量的等待時間超過該第一時間門檻值(T2)時，使用基於流量偵測模組(5)分析該流量，並產生一第一輸出概率；
當該流量的等待時間未超過該第一時間門檻值(T2)時，判斷該流量的持續時間是否超過一第二時間門檻值(T3)；
當該流量的持續時間超過該第二時間門檻值(T3)時，使用基於該封包偵測模組(6)分析該流量，並產生一第二輸出概率；以及
當該流量的持續時間未超過該第二時間門檻值(T3)時，判斷該流量太短而無法使用該基於流量偵測模組(5)及該基於封包偵測模組(6)來分析該流量，並停止對該流量的分析；
其中當該第一輸出概率被產生時，還包含步驟：使用該灰色區域模組(7)判斷是否該第一輸出概率落入一灰色區域範圍門檻範圍(T1)，且當該第一輸出概率落入該灰色區域範圍門檻範圍(T1)時，表示對於使用該基於流量偵測模組(5)對該封包進行分析的信心度不足，再次使用該基於封包偵測模組(6)重新檢測該流量。

2. 如請求項 1 所述的混合型流量與封包異常偵測系統(100)，其中該封包的屬性包含來源與目標地址、來源與目標端口或使用的協定。
3. 如請求項 1 所述的混合型流量與封包異常偵測系統(100)，其中該混合型流量與封包異常偵測系統(1)還包含一偵測標註模組(8)，由該控制模組(2)進行控制，該偵測標註模組(8)用於將該流量的該第一輸出概率或該第二輸出概率與一門檻值進行比較，以判斷該流量為正常或異常。
4. 一種混合型流量與封包異常偵測方法，透過一混合型流量與封包異常偵測系統執行，該混合型流量與封包異常偵測系統包含一控制模組(2)、一封包處理模組(3)、一流量追蹤模組(4)、一基於流量偵測模組(5)、一基於封包偵測模組(6)以及一灰色區域模組(7)，且該控制模組(2)用於控制該流量追蹤模組(4)、該基於流量偵測模組(5)、該基於封包偵測模組(6)以及該灰色區域模組(7)，其中該方法包含步驟：
藉由該封包處理模組(3)，判斷進入該混合型流量與封包異常偵測系統(100)的一封包屬於一現存流量或一新流量的一起始封包，該判斷是基於將該封包的一屬性與該現存流量的一屬性進行比對；以及針對每一流量，藉由該流量追蹤模組(4)，判斷該流量等待一個新封包到達的一時間量是否超過一第一時間門檻值(T2)，其中該第一時間門檻值(T2)是系統預設的一最大封包等待時間；
當該流量的等待時間超過該第一時間門檻值(T2)時，使用基於流量偵測模組(5)分析該流量，並產生一第一輸出概率；
當該流量的等待時間未超過該第一時間門檻值(T2)時，判斷該流量的持續時間是否超過一第二時間門檻值(T3)；
當該流量的持續時間超過該第二時間門檻值(T3)時，使用基於該封包偵測模組(6)分析該流量，並產生一第二輸出概率；以及
當該流量的持續時間未超過該第二時間門檻值(T3)時，判斷該流量太短而無法使用該基於流量偵測模組(5)及該基於封包偵測模組(6)來分析該流量，並停止對該流量的分析；
其中當該第一輸出概率被產生時，還包含步驟：使用該灰色區域模組(7)判斷是否該第一輸出概率落入一灰色區域範圍門檻範圍(T1)，且當該第一輸出概率落入該灰色區域範圍門檻範圍(T1)時，表示對於使用該基於流量偵測模組(5)對該封包進行分析的信心度不足，再次使用該基於封包偵測模組(6)重新檢測該流量。
5. 如請求項 4 所述的混合型流量與封包異常偵測方法，其中該封包的屬性包含來源與目標地址、來源與目標端口或使用的協定。
6. 如請求項 4 所述的混合型流量與封包異常偵測方法，其中還包含步驟：藉由該控制模組(2)控制一偵測標註模組(8)，將該流量的該第一輸出概率或該第二輸出概率與一門檻值進行比較，以判斷該流量為正常或異常。

圖式簡單說明

圖 1 是本發明一實施例的混合型流量與封包異常偵測系統的系統架構圖。
圖 2 是本發明一實施例的混合型流量與封包異常偵測方法的主要步驟流程圖。
圖 3 是本發明一實施例的封包處理程序的步驟流程圖。
圖 4 是本發明一實施例的運作階段處理程序的步驟流程圖。
圖 5 是本發明一實施例的流量檢查程序的步驟流程圖。
圖 6 是本發明一實施例的標註程序的步驟流程圖。

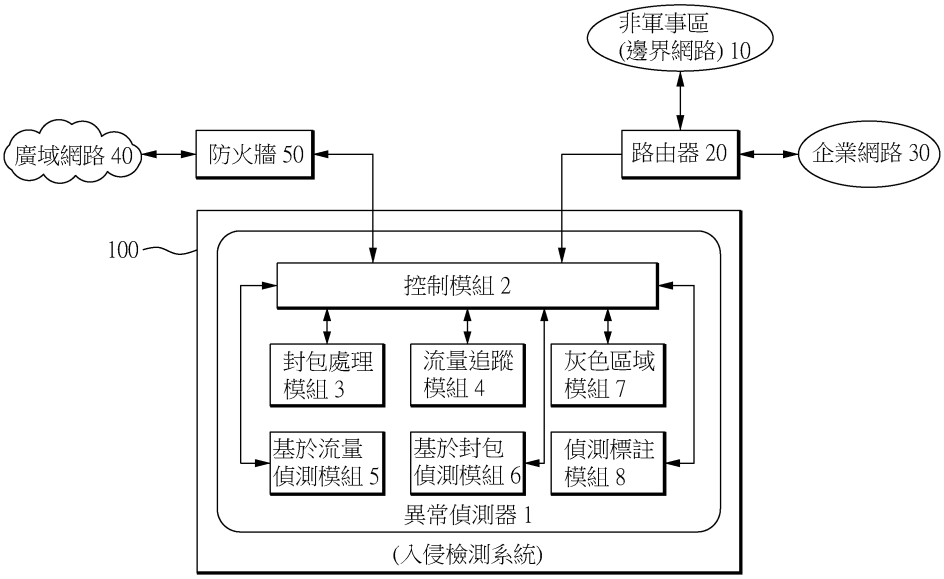
非軍事區
(邊界網路) 10
廣域網路 40
防火牆 50
路由器 20
企業網路 30
100
控制模組 2
封包處理
模組 3
流量追蹤
模組 4
灰色區域
模組 7
基於流量
偵測模組 5
基於封包
偵測模組 6
偵測標註
模組 8
異常偵測器 1
(入侵檢測系統)

圖1

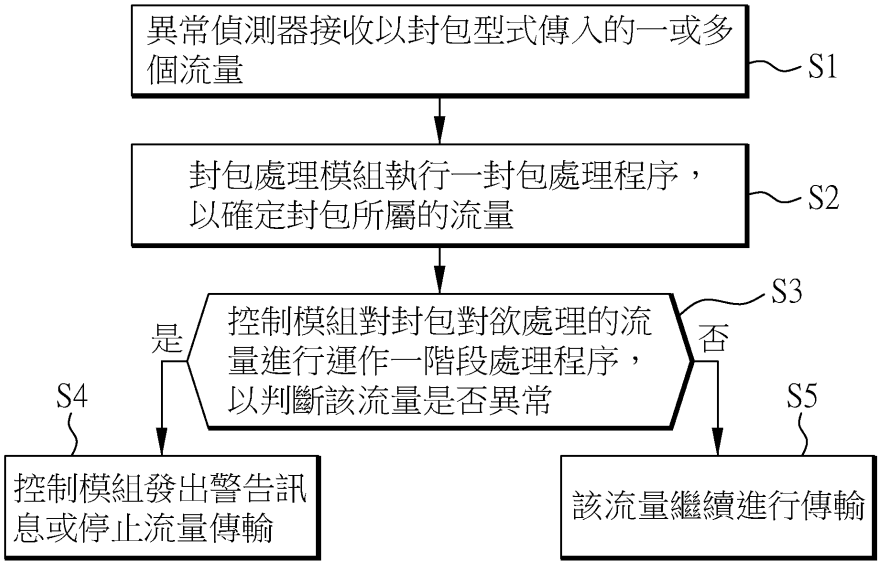
異常偵測器接收以封包型式傳入的一或多個流量
S1
封包處理模組執行一封包處理程序，以確定封包所屬的流量
S2
控制模組對封包對欲處理的流量進行運作一階段處理程序，以判斷該流量是否異常
S3
是
否
S4
S5
控制模組發出警告訊息或停止流量傳輸
該流量繼續進行傳輸

圖2

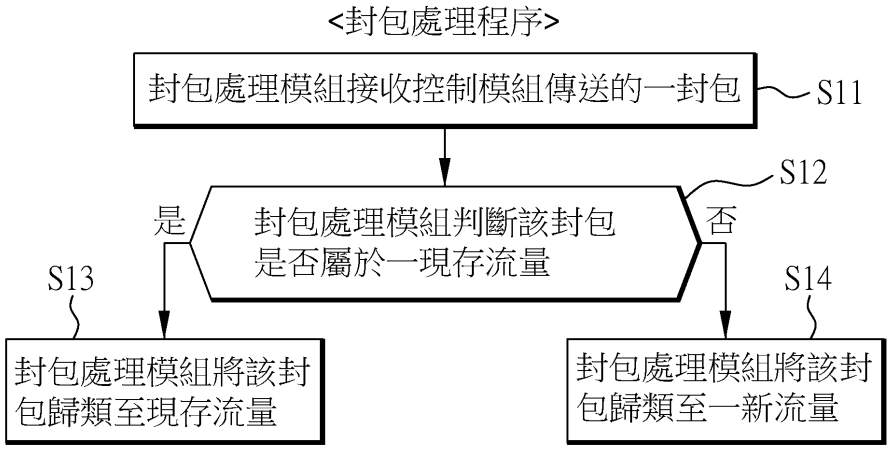
<封包處理程序>
封包處理模組接收控制模組傳送的一封包
S11
S12
是
封包處理模組判斷該封包是否屬於一現存流量
否
S13
S14
封包處理模組將該封包歸類至現存流量
封包處理模組將該封包歸類至一新流量

圖3

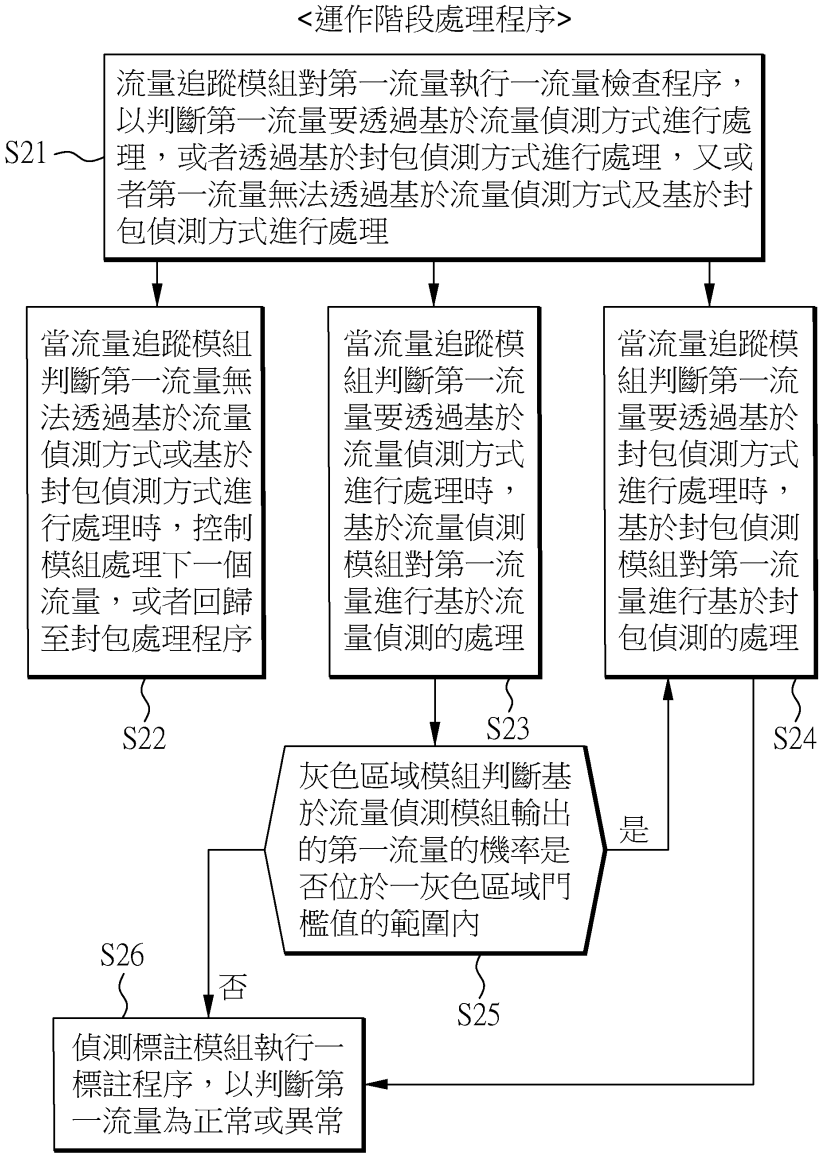
<運作階段處理程序>
流量追蹤模組對第一流量執行一流量檢查程序，以判斷第一流量要透過基於流量偵測方式進行處理，或者透過基於封包偵測方式進行處理，又或者第一流量無法透過基於流量偵測方式及基於封包偵測方式進行處理
S21
當流量追蹤模組判斷第一流量無法透過基於流量偵測方式或基於封包偵測方式進行處理時，控制模組處理下一個流量，或者回歸至封包處理程序
當流量追蹤模組判斷第一流量要透過基於流量偵測方式進行處理時，基於流量偵測模組對第一流量進行基於流量偵測的處理
當流量追蹤模組判斷第一流量要透過基於封包偵測方式進行處理時，基於封包偵測模組對第一流量進行基於封包偵測的處理
S22
S23
S24
灰色區域模組判斷基於流量偵測模組輸出的第一流量的機率是否位於一灰色區域門檻值的範圍內
是
否
S25
S26
偵測標註模組執行一標註程序，以判斷第一流量為正常或異常

圖4

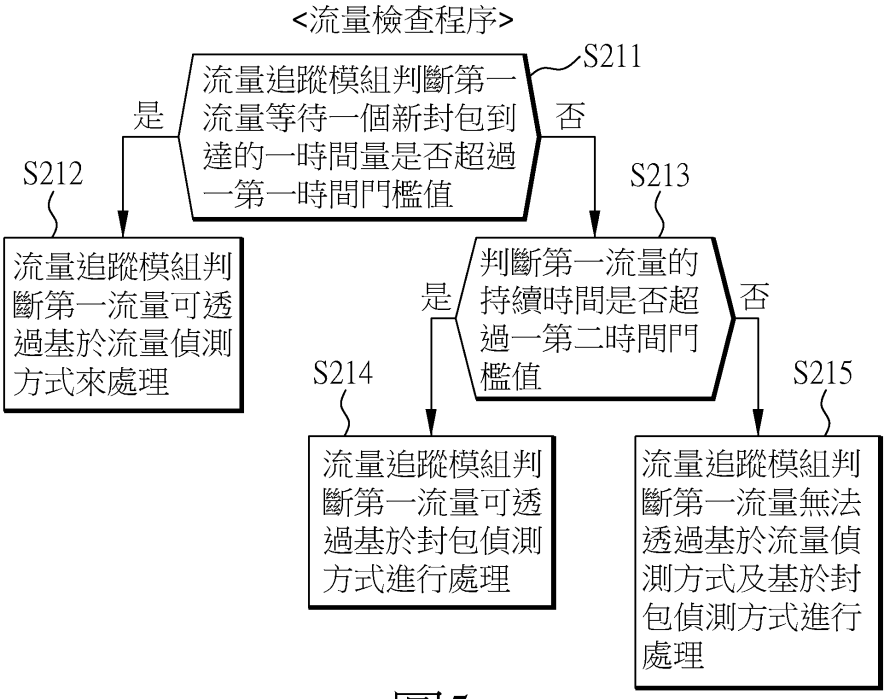
<流量檢查程序>
流量追蹤模組判斷第一流量等待一個新封包到達的一時間量是否超過一第一時間門檻值
S211
是
否
S212
流量追蹤模組判斷第一流量可透過基於流量偵測方式來處理
S213
判斷第一流量的持續時間是否超過一第二時間門檻值
是
否
S214
流量追蹤模組判斷第一流量可透過基於封包偵測方式進行處理
S215
流量追蹤模組判斷第一流量無法透過基於流量偵測方式及基於封包偵測方式進行處理

圖5

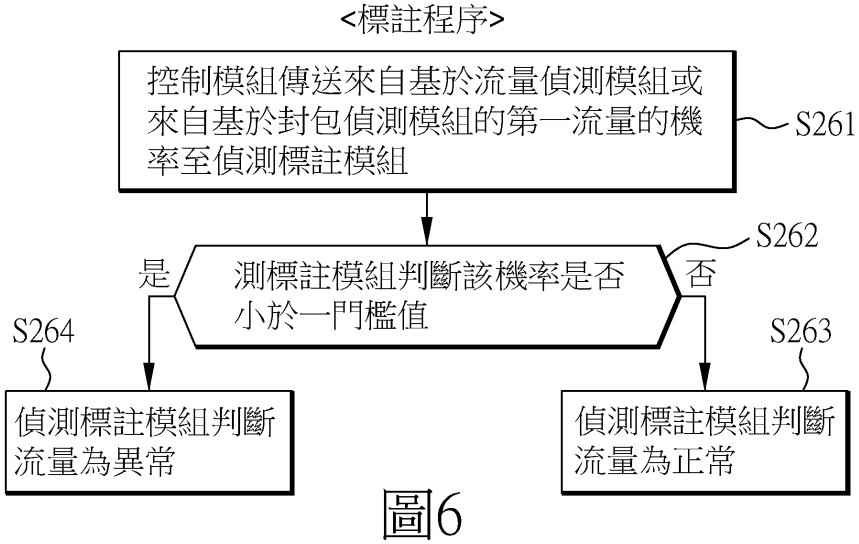
<標註程序>
控制模組傳送來自基於流量偵測模組或來自基於封包偵測模組的第一流量的機率至偵測標註模組
S261
S262
是
測標註模組判斷該機率是否小於一門檻值
否
S264
偵測標註模組判斷流量為異常
S263
偵測標註模組判斷流量為正常

圖6