(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 201031141 A1
(43)公開日： 中華民國 99 (2010) 年 08 月 16 日

(21)申請案號：098103466 (22)申請日： 中華民國 98 (2009) 年 02 月 04 日
(51)Int. Cl.： *H04L12/26 (2006.01)* *H04L29/06 (2006.01)*
(71)申請人：國立臺灣大學 (中華民國) NATIONAL TAIWAN UNIVERSITY (TW)
臺北市大安區羅斯福路 4 段 1 號
(72)發明人：楊祝晉 YANG, JHU JIN (TW) ；王勝德 WANG, SHENG DE (TW)
(74)代理人：陳昭誠
申請實體審查：有 申請專利範圍項數：14 項 圖式數：4 共 29 頁

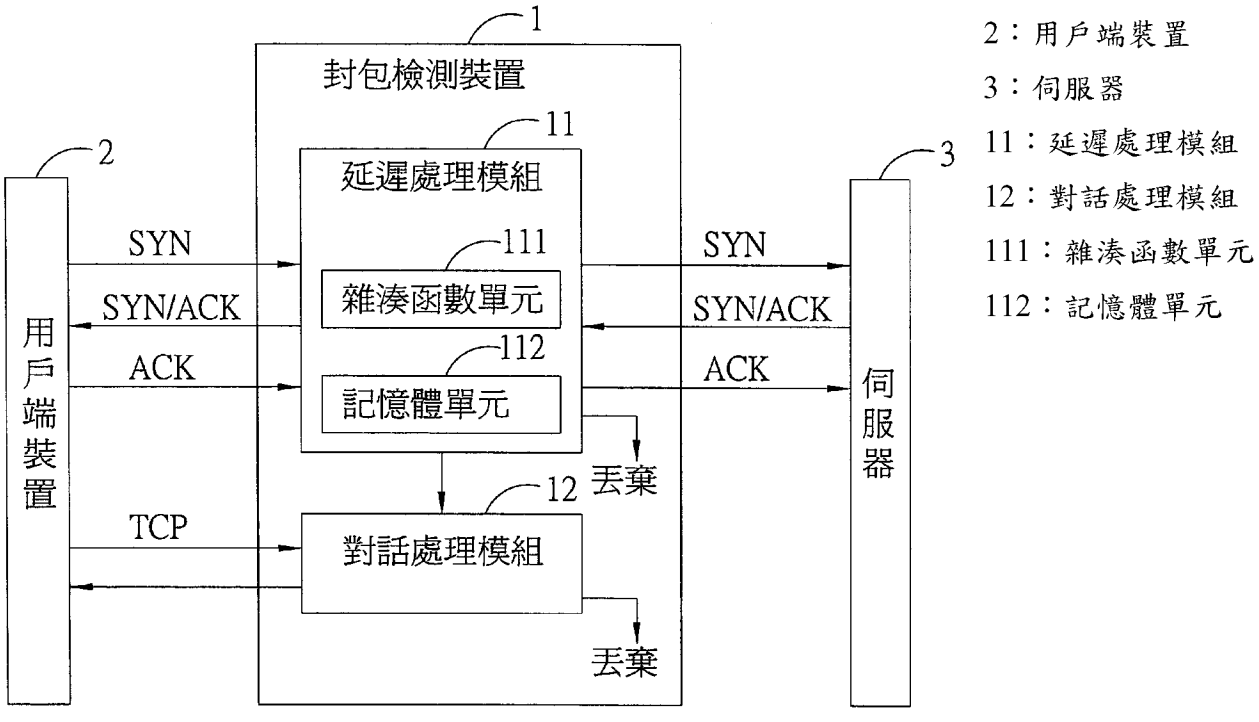
(54)名稱

封包檢測裝置及方法

PACKETS INSPECTION DEVICE AND METHOD

(57)摘要

一種封包檢測裝置及方法，係應用於擷取封包之網路設備中，其透過延遲處理模組於 TCP 層交握時，對所接收之封包進行儲存、比對以及篩選。首先，由延遲處理模組之雜湊函數(Hashing Function)單元將封包的標頭資訊轉換為雜湊函數值，接著，與延遲處理模組之記憶體單元中的資料進行雜湊函數值比對，若記憶體單元中所儲存之資料與該雜湊函數單元所轉換之雜湊函數值不相同，則將該雜湊函數值存入該記憶體單元以建立一對話連線，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值相同，則進行封包狀態比對與封包篩選，再經由對話處理模組依據該延遲處理模組所篩選之封包建立傳輸連線。據此，可快速檢測封包狀態、減少佔用記憶體空間以及降低成本。



六、發明說明：

【發明所屬之技術領域】

本發明係關於一種封包檢測裝置及方法，更詳而言之，係關於一種應用於擷取封包之網路設備，用以進行封包狀態檢測之封包檢測裝置及方法。

【先前技術】

傳輸控制協定(Transmission Control Protocol, TCP)以及網際網路協定(Internet Protocol, IP)為網際網路的重要通訊協定，可使不同的電腦設備與作業環境透過通訊協定來互通信息，而資料在 TCP/IP 上是以封包的形式來傳送。

於 TCP 層進行資料傳輸時，必須先建立起兩者之間的連線關係，TCP 層連線的建立是透過帶有連線控制訊息的封包在兩端主機間傳遞，再藉由 TCP 封包標頭(Header)資訊和狀態機制(State machine)的檢測，經一番交談(Session)後，發送端與接收端進入連線狀態。經由此連線請求、連線確認、連線成功的程序，便形成了三方交握(3-way handshaking)。

隨著網路攻擊的數量與複雜度與日俱增，其中最流行的網路攻擊之一為 SYN(Synchrony)、SYN/ACK、ACK(Acknowledge) DoS attack(拒絕服務攻擊)，例如 SYN 洪流攻擊(Flooding Attack)，伺服器在接收到用戶端發送之 SYN 封包後發出 SYN/ACK 封包，卻一直無法收到用戶端的 ACK 封包，在這種情況下伺服器會再次發送 SYN/ACK 封包給用戶端並等待一段時間後丟棄(drop)這個未完成的

連接，如果惡意地大量發送 SYN 封包，伺服器端將為了維護一個非常大的半連線狀態而消耗 CPU 資源和記憶體。

目前習知技術提出了狀態檢查機制 (Stateful Inspection Module Architecture)，其方法為紀錄封包流的狀態，於封包紀錄表中搜尋封包流的狀態紀錄，以判斷進入的封包是否為正常的封包，而搜尋資料的方法分為下列三種：一種從資料的第 1 筆資料開始比較，從頭到尾以確認資料是否存在，例如：線性搜尋法，一種為使用樹狀結構搜尋法，例如樹狀資料結構(AVL Tree)，另一種為在硬體方面的改善，例如增加一個內容定址記憶體(Content Address Momery,CAM)。

然而，上述習知技術存在以下問題：

(1) 封包檢測速度慢。於檢測封包狀態時，利用線性搜尋法搜尋連線紀錄，使插入封包狀態和更新封包狀態時所搜尋的時間與連線紀錄成正比。

(2) 佔用記憶體空間多。利用樹狀結構搜尋法可加快速度，相對而言，也佔用了記憶體儲存空間。

(3) 成本高。利用內容定址記憶體雖可快速地進行封包檢測以及減少佔用記憶體空間，但是缺點為成本昂貴而無法普及使用。

綜上所述，如何能提供一種封包檢測裝置及方法，能快速檢測封包狀態、減少佔用記憶體空間以及降低成本，以抵擋網路惡意封包攻擊，遂成為目前亟待解決的課題。

【發明內容】

鑑於上述習知技術之缺點，本發明提供一種封包檢測裝置，係應用於擷取封包之網路設備，該封包檢測裝置係包括：延遲處理模組，係用以於TCP層交握時，對該封包進行儲存、比對以及篩選，該延遲處理模組係包括用以將資訊轉換為雜湊函數值之雜湊函數單元與用以儲存該雜湊函數值之記憶體單元；以及對話處理模組，係依據該延遲處理模組所篩選之封包建立一傳輸連線，其中，該延遲處理模組之雜湊函數單元將該封包之標頭資訊轉換為雜湊函數值並進行雜湊函數值比對，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值不相同，則將該雜湊函數值存入該記憶體單元以建立一對話連線，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值相同，則進行封包狀態比對與封包篩選。

本發明另提供一種封包檢測方法，係應用於具有延遲處理模組與對話處理模組之封包檢測裝置，該封包檢測方法係包括以下步驟：(1)令該延遲處理模組於TCP層交握時透過雜湊函數單元將所接收到封包之標頭資訊轉換為雜湊函數值並進行比對，若記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值不相同，進至步驟(2)，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值相同，進至步驟(3)；(2)令該延遲模組建立對話連線，進至步驟(4)；(3)將該封包與對應該封包之對話連線之狀態進行比對，若狀態不符合，則丟棄該封包，若狀態符合，則進至步驟(4)；以及(4)令該延遲處理模組持續進行交

握或將該封包傳至該對話處理模組以建立傳輸連線。

於一較佳態樣中，步驟(1)復包括：(1-1)將該封包之標頭資訊以雜湊函數轉換為位址值；(1-2)將該封包之標頭資訊以雜湊函數轉換為鍵值；以及(1-3)將該位址值內之資訊與該封包之鍵值進行比對，若該不相同，則將該封包之鍵值存入該位址值，若相同，則進行封包狀態比對以及封包篩選。

相較於習知技術，本發明利用設置於封包檢測裝置之延遲處理模組之雜湊函數單元將封包標頭資訊轉換為雜湊函數值，並與延遲處理模組之記憶體單元進行雜湊函數值比對，再進行與對應該封包之對話連線之狀態進行比對，經由對話處理模組依據該延遲處理模組所篩選之封包建立傳輸連線，進而抵擋網路惡意封包攻擊。

因此，本發明之封包檢測裝置及方法具有增加封包狀態檢測速度、減少記憶體佔用空間以及降低成本之功效，得以解決習知技術中封包檢測之既有的缺點。

【實施方式】

以下係藉由特定的具體實施例說明本發明之實施方式，熟悉此技術之人士可由本說明書所揭示之內容輕易地了解本發明之其他優點與功效。本發明亦可藉由其他不同的具體實施例加以施行或應用，本說明書中的各項細節亦可基於不同觀點與應用，在不悖離本發明之精神下進行各種修飾與變更。

以下實施例係近一步詳細說明本發明之觀點，但並非

以任何觀點限制本發明之範疇。

請參閱第 1 圖，係表示本發明之封包檢測裝置之架構示意圖。如圖所示，本發明之封包檢測裝置 1 係設置於擷取封包之網路設備(在此未予以圖示)，其中，網路設備係作為電腦設備連接網際網路的媒介。於本實施例中，用戶端裝置 2 與伺服器 3 透過網路設備連接網際網路，而網路設備可為交換設備、傳輸設備、寬頻接取設備、區域網路設備、寬頻網路應用設備及/或用戶端設備。

用戶端設備可為數據機(Modem)，有線區域網路設備可為網卡(NIC)或集線器(Hub)，交換設備可為交換機(switch)或路由器（router）。

本發明之封包檢測裝置 1 包括延遲處理模組 11 以及對話處理模組 12。

延遲(Pending)處理模組 11，係用以於傳輸控制協定 TCP 層進行三方交握時，對該封包進行儲存、比對以及篩選。

對話(Session)處理模組 12，係依據延遲處理模組 11 所篩選之封包建立傳輸連線。

延遲處理模組 11 復包括雜湊函數單元 111 以及記憶體單元 112。

雜湊函數單元 111，係用以將資訊轉換為雜湊函數(Hashing function)值。

記憶體單元 112，係用以儲存該雜湊函數值。

具體實施時，首先，延遲處理模組 11 接收到用戶端

裝置 2 所發送之一 SYN 封包，利用存取規則表(Access Control List, ACL)(在此未予以圖式)判斷是否接受該 SYN 封包，若不接收則丟棄(Drop)。接受該 SYN 封包後，雜湊函數單元 111 將該 SYN 封包之標頭資訊轉換為雜湊函數值並進行雜湊函數值比對，若記憶體單元 112 中無相同之雜湊函數值，則將該 SYN 封包存入記憶體單元 112 中以建立對話連線，若記憶體單元 112 中有相同之雜湊函數值，則將該 SYN 封包傳予伺服器 3 並將連線狀態更新為等待 SYN/ACK 封包之狀態。

接著，延遲處理模組 11 在接收到伺服器 3 所發送之 SYN/ACK 封包，雜湊函數單元 111 將該 SYN/ACK 封包之標頭資訊轉換為雜湊函數值並進行雜湊函數值比對，若記憶體單元 112 中無相同之雜湊函數值，則將該 SYN/ACK 封包丟棄，若記憶體單元 112 中有相同之雜湊函數值，則將 SYN/ACK 封包傳予用戶端裝置 2 並將連線狀態更新為等待 ACK 封包之狀態。

最後，延遲處理模組 11 在接收到用戶端裝置 2 所發送之 ACK 封包，雜湊函數單元 111 將該 ACK 封包之標頭資訊轉換為雜湊函數值並進行雜湊函數值比對，若記憶體單元 112 中無相同之雜湊函數值，則丟棄該 ACK 封包，若記憶體單元 112 中有相同之雜湊函數值，則將該 ACK 封包傳至對話處理模組 12 以建立傳輸連線，並於 TCP 層傳輸結束時，將該 ACK 封包從對話處理模組 12 中刪除。

其中，若進行比對的時間值(Timestamp)超過一特定值

(Threshold)，則刪除逾時的封包以接受新的封包。

請參閱第 2A 圖，其係本發明之封包檢測裝置之雜湊函數單元以及記憶體單元之進行雜湊函數值比對之示意圖，如圖所示，雜湊函數單元 41 係包括第一函數轉換器 411、第二函數轉換器 412 以及比對器 413，記憶體單元 42 係用以儲存位址值 421、位址值之資訊 422a 以及 422b，其中，資訊 422a 與資訊 422b 之資訊係不相同，且每一筆資訊代表一個封包連線紀錄。

封包之標頭資訊 40 為來源 IP、來源 port、目的地 IP 以及目的地 port。

第一函數轉換器 411，係用以將該封包之標頭資訊 40 以一雜湊函數轉換為位址值。

第二函數轉換器 412，係用以將該封包之標頭資訊 40 以另一雜湊函數轉換為鍵值。

比對器 413，係用以取出記憶體單元 42 中之位址值 421 內之資訊 422a 以及 422b 與該封包之鍵值依序進行比對，若不相同，則將該鍵值存入該位址值 421，若相同，則進行封包狀態比對以及封包篩選。

本發明之封包檢測裝置復包括內容定址記憶體 43(content addressable memory, CAM)，係用以於記憶體單元 42 中之位址值 421 已滿時儲存該封包之鍵值。

具體實施時，首先，延遲處理模組於接到一封包時，第一函數轉換器 411 將封包之標頭資訊 40 轉換為位址值，且第二函數轉換器 412 將封包之標頭資訊 40 轉換為鍵值，

接著，由比對器 413 於記憶體單元 42 中找到符合該封包之位址值 421，並將封包之鍵值與位址值 421 內之資訊 422a 及 422b 進行比對，若資訊 422a 及資訊 422b 之其中之一資訊是空的且另一資訊是不相同的，則將封包之鍵值存入該位址值 421 內，若皆不相同且資訊 422a 及資訊 422b 已滿時，將該封包之鍵值存入內容定址記憶體 43 中，以等待接收下一個封包，若資訊 422a 及資訊 422b 之其中之一資訊與封包之鍵值相同時，則進行封包狀態之比對，若狀態符合，則令延遲處理模組持續進行交握或將該封包傳至對話處理模組以建立傳輸連線，若狀態不符合，則將該封包丟棄。

上述封包狀態之比對方法為狀態追蹤(state tracking)、封包存活期間(Time To Live, TTL)追蹤、以及序列追蹤(Sequence tracking)及/或確認追蹤(Acknowledge tracking)。

請參閱第 2B 圖，係用以表示本發明之封包檢測裝置之雜湊函數元件之轉換鍵值示意圖。本發明之封包檢測裝置之較佳態樣為第二函數轉換器 412 復包括複數個雜湊函數元件 4121，於本實施例中，H_1 至 H_4 為雜湊函數，雜湊函數元件 4121 係用以將封包之標頭資訊 40 以複數個相異之雜湊函數轉換為鍵值。

具體實施時，首先，延遲處理模組於接到一封包時，第一函數轉換器 411 將封包之標頭資訊 40 轉換為位址值，且雜湊函數元件 4121 利用雜湊函數 H_1 至 H_4 將封包之標頭

資訊 40 轉換為鍵值 1 至鍵值 4。

接著，由比對器 41 搜尋到符合該封包之位址值之記憶體單元 42 的位址值 421，並取出位址值 421 中之資訊 422a 及資訊 422b 進行比對。

將封包之鍵值 1 與資訊 422a 內之第一筆資料以及與資訊 422b 內之第一筆資料進行比對，若符合，則進行該封包之狀態資料比對，若不符合則將該封包之鍵值存入位址值 421 內或於位址值 421 已滿時存入內容定址記憶體 43，若封包之狀態比對符合，則持續進行交握或進行傳輸連線，若封包之狀態比對不符合，則將該封包之鍵值 2 與資訊 422a 內之第二筆資料與資訊 422b 內之第二筆資料進行比對，以此類推，直到鍵值 4 比對完成且封包狀態也不符合時，將該封包丟棄。

因為雜湊函數 H_1 至 H_4 具有獨立性(independence)，同一封包以不同之雜湊函數不會計算出相同之位址值 421，但是不同之封包以相同之雜湊函數則可能會計算出相同之位址值 421，因此本發明於一記憶體單元 42 之位址值 421 內設有多個資訊 422a~422b，而每一筆資訊 422 代表一個封包紀錄，以供封包之鍵值比對，以降低因不同的封包對應到同一位址值 421 而無法連線之機率，並在位址值 421 之資訊 422 內設有多筆資料(在此為予以圖示)，以供該封包於鍵值 1 比對成功後，且在進行封包狀態比對不符合時，取出該封包之鍵值 2 再次與資訊 422 之內容進行比對，以降低了無法連線之機率，因此，本發明之檢測裝置加快

了封包檢測之速度以及減少記憶體佔有之空間，此外，於本發明之封包檢測裝置設置有一內容定址記憶體43，由於內容定址記憶體 43 具有快速比對雜湊函數值之特性但相對地價格昂貴，所以本發明僅於該記憶體單元 42 中之位址值421已滿時儲存該封包之鍵值且於記憶體單元42中搜尋不到相同鍵值時搜尋內容定址記憶體43，以更快速地進行封包檢測以及維持低成本之功效。

請參閱第 3A 圖，其用以表示本發明之封包檢測方法之流程圖，該封包檢測方法係應用於具有延遲處理模組與對話處理模組之封包檢測裝置。

如圖所示，本發明之封包檢測方法係包括以下步驟：首先執行步驟 S21，令該延遲處理模組於 TCP 層交握時透過雜湊函數單元將所接收到封包之標頭資訊轉換為雜湊函數值並進行比對，其中該雜湊函數值為位址值與鍵值。接著進至步驟 S22。

於步驟 S22 中，該記憶體單元中是否具有相同之雜湊函數值，若否，則進至步驟 S23，若是，則進至步驟 S24。

於步驟 S23 中，令該延遲模組建立對話連線，接著返回步驟 S21 對下一封包進行檢測。

於步驟 S24 中，將該封包與對應該封包之對話連線之狀態進行比對。接著進至步驟 S25。

於步驟 S25 中，該封包是否符合對應該封包之對話連線之狀態，若是，則進至步驟 S26，若否，則進至 S27。

於步驟 S26 中，令該延遲處理模組持續進行交握或將

該封包傳至該對話處理模組以建立傳輸連線，其中，於 TCP 層傳輸結束時，將該封包於該對話處理模組中刪除。

於步驟 S27 中，丟棄該封包。

請參閱第 3B 圖，為前述步驟 S21 與步驟 S22 之詳細運作流程，用以表示本發明之封包檢測方法中進行雜湊函數值比對之流程圖。如圖所示，首先執行步驟 S31，將該封包之標頭資訊以雜湊函數轉換為位址值。接著進至步驟 S32。

於步驟 S32 中，將該封包之標頭資訊以雜湊函數轉換為鍵值。接著進至步驟 S33。

於步驟 S33 中，將該位址值內之資訊與該封包之鍵值進行比對。接著進至步驟 S34。

於步驟 S34 中，該位址值內之資訊是否與該封包之鍵值相同，若是，則進至步驟 S35，若否，則進至步驟 S36。

於步驟 S35 中，進行封包狀態比對以及封包篩選。

於步驟 S36 中，將該封包之鍵值存入該位址值。

透過上述實施例得以瞭解，本發明之封包檢測方法利用雜湊函數將封包之標頭資訊轉換成位址值及鍵值，以於記憶體單元中進行快速比對，俾增加封包檢測速度以及減少記憶體佔用空間，進而抵擋網路惡意封包攻擊。

請參閱第 4 圖，其係本發明之封包檢測裝置及方法之應用實施例示意圖。於本實施例中，本發明之封包檢測裝置係加載於擷取封包之網路設備，係用以當一封包進入具有延遲處理模組及對話處理模組之封包檢測裝置時，對該

封包之儲存、比對及篩選。

於本發明之封包檢測裝置收到一封包時，將該封包之標頭資訊轉換為位址值以及鍵值，以定址到延遲處理模組之記憶體單元之位址值，再對該位址值內之資訊進行比對，若該延遲處理模組之記憶體單元中無對應於該封包之資訊，則於該對話處理模組中再進行比對，若無對應於該封包之資訊，則判斷該封包是否為 SYN 封包，若否，則丟掉並紀錄該封包，若該封包為 SYN 封包，則由存取規則表判斷是否接受該封包，若不接受則丟棄並紀錄該封包，若接受則將該封包存入該延遲處理模組之記憶體單元以建立對話連線，其中，若本發明之封包檢測裝置接收到一 SYN 封包，但在該延遲處理模組之記憶體單元中尚有未完成之對應於該封包之交握對話，則丟棄及紀錄該封包。

若於該延遲處理模組之記憶體單元中有對應於該封包之資訊，則再於該對話處理模組之記憶體單元中進行比對，若於該對話處理模組之記憶體單元中有對應於該封包之資訊，則丟棄及紀錄該封包，若於該對話處理模組之記憶體單元中無對應於該封包之資訊，則進行封包狀態比對，若比對不符合則丟棄及紀錄該封包，若比對符合，則判斷該封包為 SYN/ACK 封包或 ACK 封包，若兩者都不是，則丟棄及紀錄該封包，若為 SYN/ACK 封包，則令該延遲處理模組持續進行交握，若為 ACK 封包，則將該封包從該延遲處理模組之記憶體單元中刪除並存入該對話處理模組之記憶體單元以建立傳輸連線。

若於該延遲處理模組之記憶體單元中無對應於該封包之資訊且於該對話處理模組之記憶體單元中有對應於該封包之資訊，則進行封包狀態比對，若該封包狀態符合，則更新對應於該封包之對話連線之狀態，若該封包狀態不符合則丟棄及紀錄該封包。

因此，透過前述之封包檢測裝置與方法，可達到以下功效：

(1) 增加封包檢測速度。透過利用雜湊函數將封包之標頭資訊轉換成位址值及鍵值且並進行與記憶體中之資訊比對，解決了習知技術中線性比對之時間過長的缺點而加快封包檢測之速度。

(2) 減少記憶體佔用空間。透過利用雜湊函數將封包之標頭資訊轉換成位址值及鍵值並進行比對，解決了習知技術中樹狀比對之佔用記憶體空間的缺點。

(3) 降低成本。透過利用雜湊函數將封包之標頭資訊轉換成位址值及鍵值且進行比對以儲存封包狀態建立連線，只於延遲處理模組之記憶體單元已滿時將封包之鍵值存入內容定址記憶體，解決了習知技術中以高價格之內容定址記憶體作為主記憶體之缺點。

上述實施例僅例示性說明本發明之原理及功效，而非用於限制本發明。任何熟習此項技術之人士均可在不違背本發明之精神及範疇下，對上述實施例進行修飾與改變。因此，本發明之權利保護範圍，應如後述之申請專利範圍所列。

【圖式簡單說明】

第 1 圖係本發明之封包檢測裝置之架構示意圖；

第 2A 圖係本發明之封包檢測裝置中雜湊函數單元以及記憶體單元進行雜湊函數值比對之示意圖；

第 2B 圖係本發明之封包檢測裝置中雜湊函數元件進行鍵值轉換之示意圖；

第 3A 圖係本發明之封包檢測方法之流程圖；

第 3B 圖係本發明之封包檢測方法中進行雜湊函數值比對之流程圖；以及

第 4 圖係本發明之封包檢測裝置及方法之應用實施例示意圖。

【主要元件符號說明】

1	封包檢測裝置
11	延遲處理模組
111	雜湊函數單元
112	記憶體單元
12	對話處理模組
2	用戶端裝置
3	伺服器
40	封包之標頭資訊
41	雜湊函數單元
411	第一函數轉換器
412	第二函數轉換器
4121	雜湊函數元件

413	比對器
42	記憶體單元
421	位址值
422a~422b	位址值之資訊
43	內容定址記憶體
S21~S27	步驟
S31~S36	步驟

201031141

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：98103466

※申請日：98.02.04 ※IPC分類：H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

封包檢測裝置及方法

PACKETS INSPECTION DEVICE AND METHOD

二、中文發明摘要：

一種封包檢測裝置及方法，係應用於擷取封包之網路設備中，其透過延遲處理模組於TCP層交握時，對所接收之封包進行儲存、比對以及篩選。首先，由延遲處理模組之雜湊函數(Hashing Function)單元將封包的標頭資訊轉換為雜湊函數值，接著，與延遲處理模組之記憶體單元中的資料進行雜湊函數值比對，若記憶體單元中所儲存之資料與該雜湊函數單元所轉換之雜湊函數值不相同，則將該雜湊函數值存入該記憶體單元以建立一對話連線，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值相同，則進行封包狀態比對與封包篩選，再經由對話處理模組依據該延遲處理模組所篩選之封包建立傳輸連線。據此，可快速檢測封包狀態、減少佔用記憶體空間以及降低成本。

三、英文發明摘要：

The invention provides a device and a method for inspecting packets applicable to network systems, characterized by using a delay processing module for storage, comparison and selection of received packets in hold of the TCP layer. The inspection method comprises converting packet title information into a hashing function value by a hashing function unit of the delay processing module; comparing the converted hashing function value with the data stored in a memory unit of the delay processing module, wherein if the stored data is found to be inconsistent with the hashing function value converted by the hashing function unit, the hashing function value is stored into the memory unit for establishing an online conversation, and if the stored data is consistent with the converted hashing function value, comparing packets status and selecting packets for establishing online transmission according to selected packets, thereby effectively inspecting packets status for the reduction of costs and the memory space as a result.

七、申請專利範圍：

1. 一種封包檢測裝置，係應用於擷取封包之網路設備，用以對網路封包進行狀態檢測，該封包檢測裝置係包括：

延遲處理模組，係用以於 TCP 層交握時，對該封包進行儲存、比對以及篩選，該延遲處理模組包括用以將資訊轉換為雜湊函數值之雜湊函數單元與用以儲存該雜湊函數值之記憶體單元，其中，該延遲處理模組之雜湊函數單元將該封包之標頭資訊轉換為雜湊函數值並進行雜湊函數值比對，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值不相同，則將該雜湊函數值存入該記憶體單元以建立一對話連線，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值相同，則進行封包狀態比對與封包篩選；以及

對話處理模組，係依據該延遲處理模組所篩選之封包建立一傳輸連線。

2. 如申請專利範圍第 1 項之封包檢測裝置，其中，該對話處理模組復包括用以將封包資訊轉換為雜湊函數值之雜湊函數單元以及用以儲存該雜湊函數值之記憶體單元。

3. 如申請專利範圍第 1 項之封包檢測裝置，其中，該延遲處理模組係依據封包狀態比對結果進行封包篩選，若狀態不符合，則丟棄該封包，若狀態符合，則使該

延遲處理模組繼續進行交握或將該封包傳予該對話處理模組以建立該傳輸連線。

4. 如申請專利範圍第 1 或 3 項之封包檢測裝置，其中，該封包狀態之比對方式為狀態追蹤、封包存活期間追蹤、以及序列追蹤及/或確認追蹤。

5. 如申請專利範圍第 1 項之封包檢測裝置，其中，該延遲處理模組依據所接收之 SYN 封包、SYN/ACK 封包或 ACK 封包進行三方交握。

6. 如申請專利範圍第 1 項之封包檢測裝置，其中，該雜湊函數單元復包括：

第一函數轉換器，係用以將該封包之標頭資訊轉換為位址值；

第二函數轉換器，係用以將該封包之標頭資訊轉換為鍵值；

比對器，係用以取出該記憶體單元中之位址值內之資訊與該封包之鍵值依序進行比對，若不相同，則將該鍵值存入該位址值，若相同，則進行封包狀態比對以及封包篩選。

7. 如申請專利範圍第 6 項之封包檢測裝置，其中，該延遲模組復包括內容定址記憶體(content addressable memory, CAM)，係用以於該記憶體單元中之位址值之資訊已滿時儲存該封包之鍵值。

8. 如申請專利範圍第 7 項之封包檢測裝置，其中，若該記憶體單元中之位址值內的雜湊函數值與該封包之鍵

值均不相同，則由該比對器取出該內容定址記憶體中的資訊進行比對。

9. 如申請專利範圍第 7 項之封包檢測裝置，其中，該第二函數轉換器係具有複數個用以將該封包之標頭資訊轉換為鍵值之雜湊函數元件。

10. 如申請專利範圍第 1 或 6 項之封包檢測裝置，其中，該封包之標頭資訊為來源 IP、來源 port、目的地 IP 以及目的地 port。

11. 一種封包檢測方法，係應用於具有延遲處理模組與對話處理模組之封包檢測裝置，該封包檢測方法係包括以下步驟：

(1)令該延遲處理模組於 TCP 層交握時透過雜湊函數單元將所接收到封包之標頭資訊轉換為雜湊函數值並進行比對，若記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值不相同，進至步驟(2)，若該記憶體單元所儲存之資料與該雜湊函數單元所轉換之雜湊函數值相同，進至步驟(3)；

(2)令該延遲模組建立一對話連線，接著返回步驟(1)對下一封包進行檢測；

(3)將該封包與對應該封包之對話連線之狀態進行比對，若狀態不符合，則丟棄該封包，若狀態符合，則進至步驟(4)；以及

(4)令該延遲處理模組持續進行交握或將該封包傳至該對話處理模組以建立傳輸連線。

12. 如申請專利範圍第 11 項之封包檢測方法，其中，步驟(1)復包括：

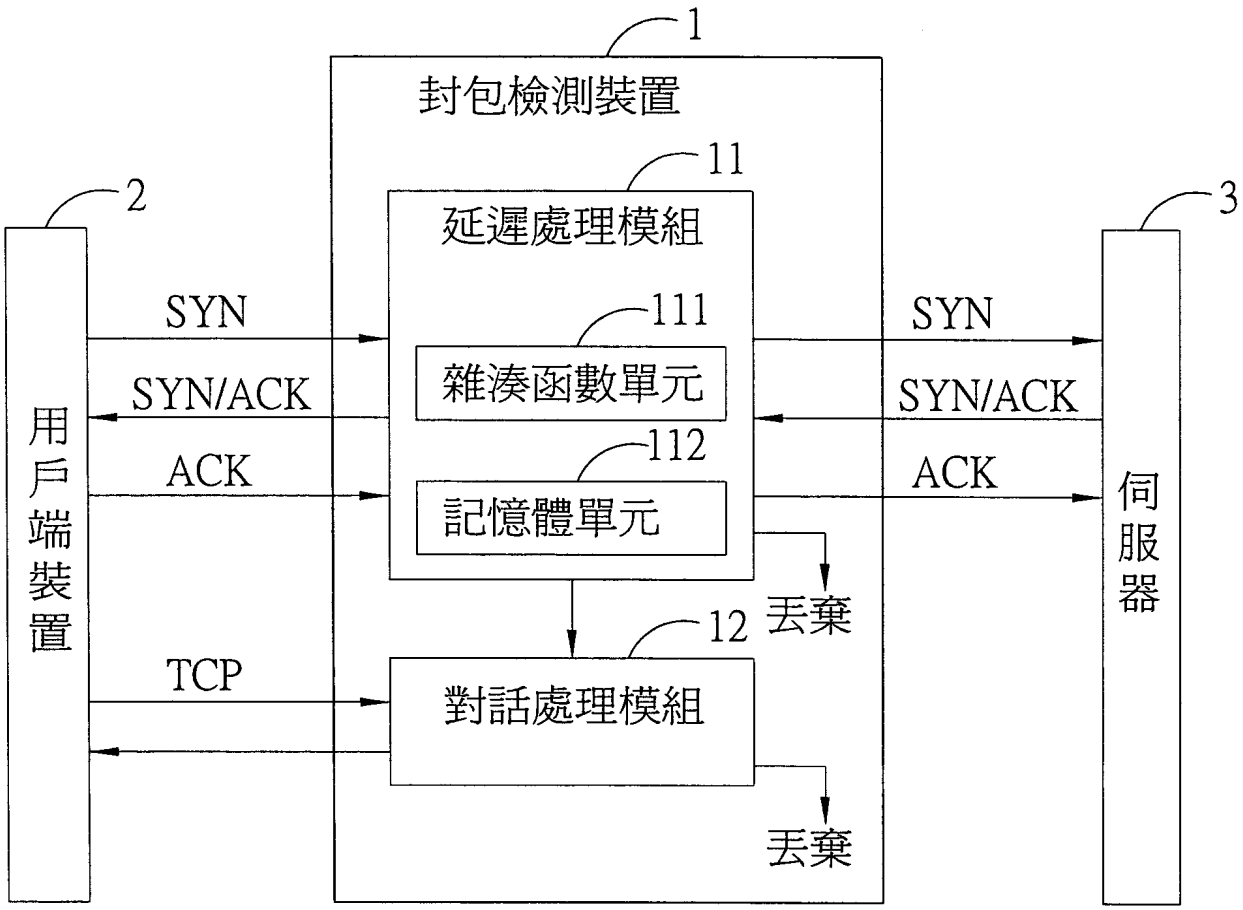
(1-1)將該封包之標頭資訊以雜湊函數轉換為位址值；

(1-2)將該封包之標頭資訊以雜湊函數轉換為鍵值；以及

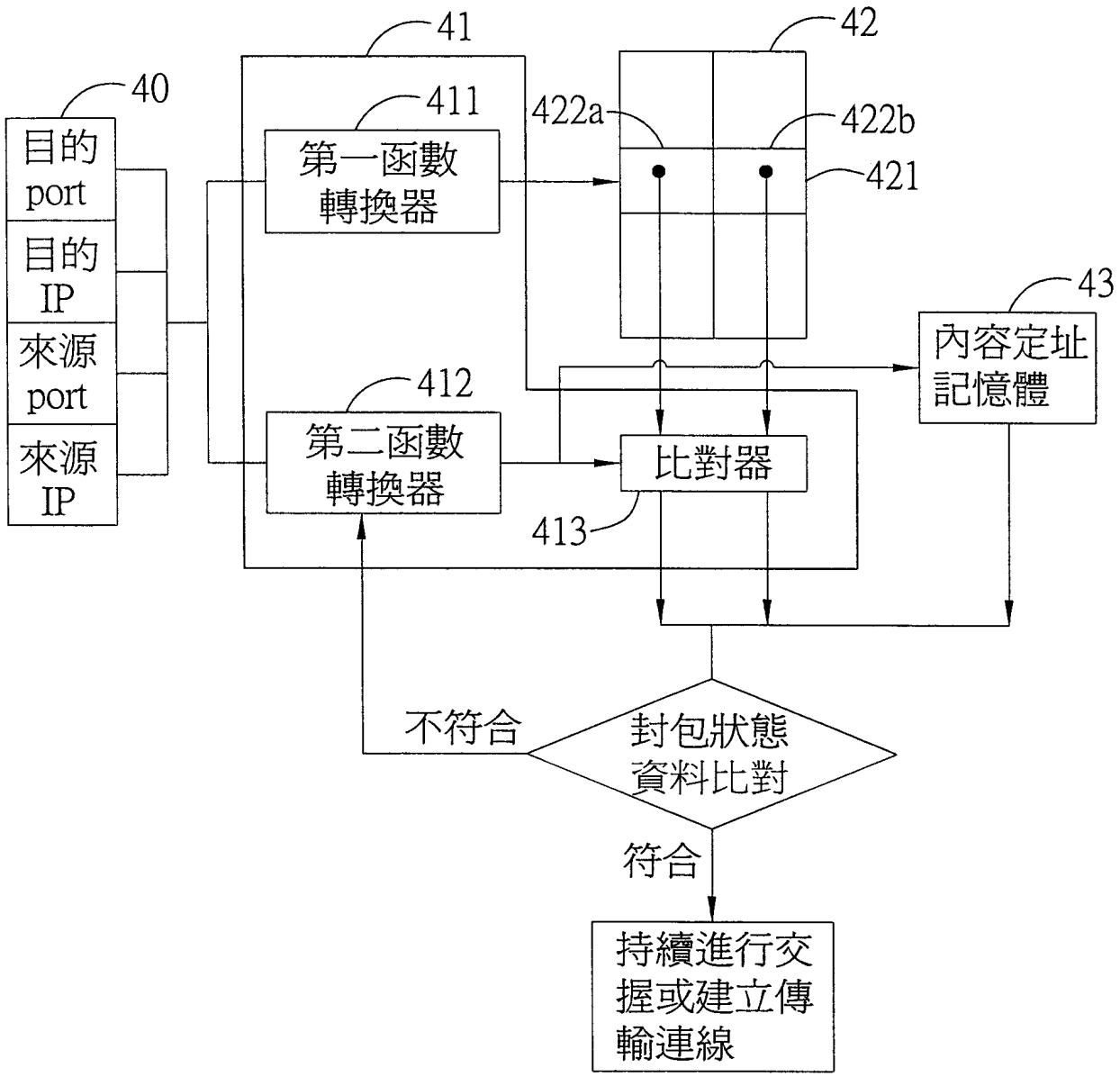
(1-3)將該位址值內之資訊與該封包之鍵值進行比對，若該不相同，則將該封包之鍵值存入該位址值，若相同，則進行封包狀態比對以及封包篩選。

13. 如申請專利範圍第 12 項之封包檢測方法，其中，於步驟(1-2)中，將封包之標頭資訊以複數個雜湊函數轉換為複數個鍵值。

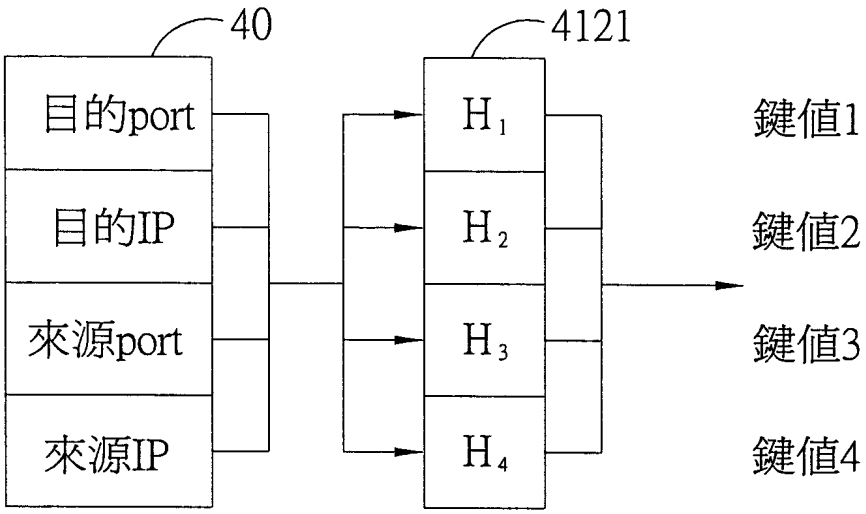
14. 如申請專利範圍第 12 項之封包檢測方法，其中，於該記憶體單元中之位址值之資訊已滿時，將該封包之鍵值儲存於內容定址記憶體。


1
封包檢測裝置
11
延遲處理模組
111
雜湊函數單元
112
記憶體單元
12
對話處理模組
2
用戶端裝置
3
伺服器
SYN
SYN/ACK
ACK
TCP
SYN
SYN/ACK
ACK
丟棄
丟棄

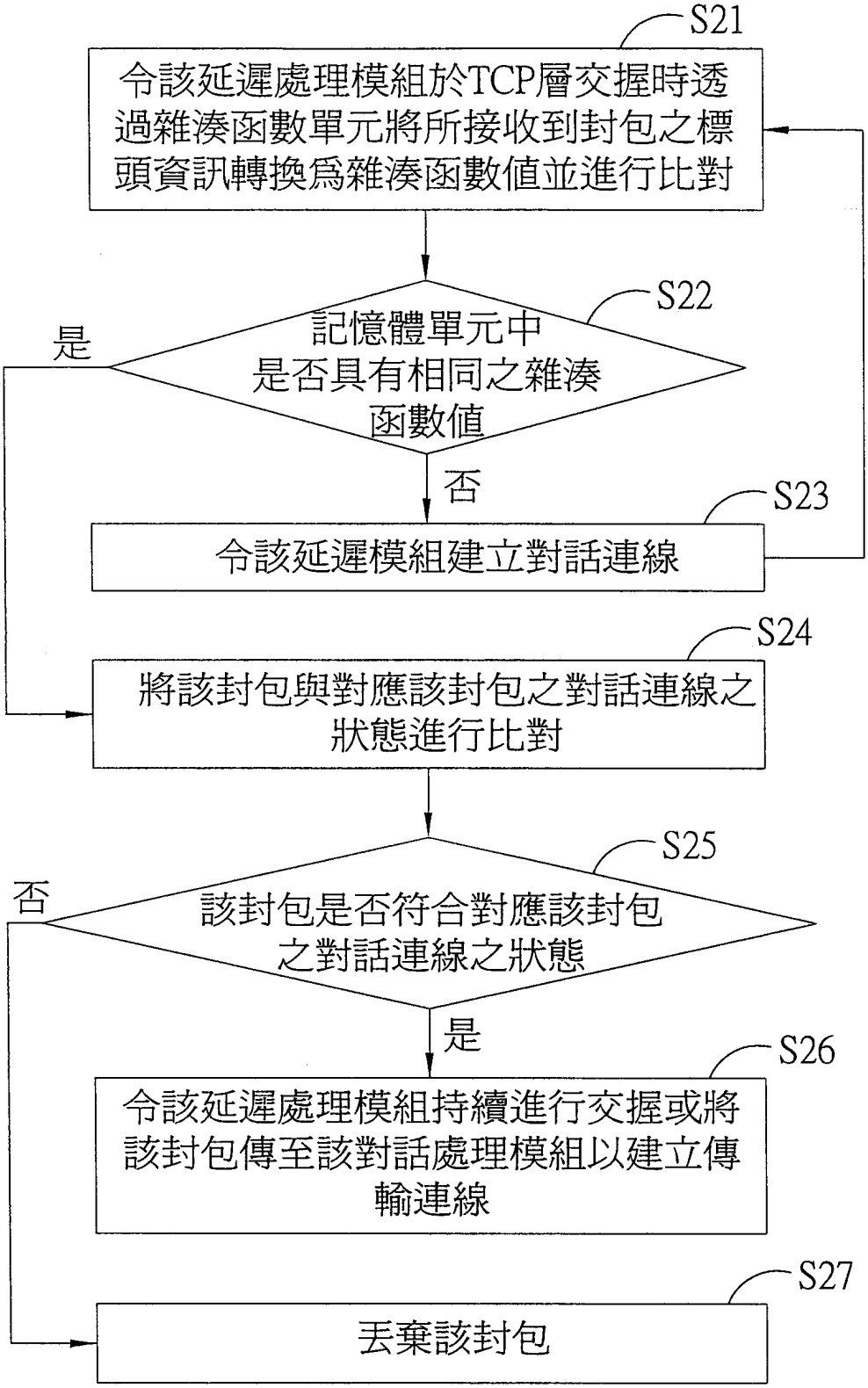
第1圖


41
42
40
411
422a
422b
目的 port
第一函數轉換器
421
目的 IP
43
來源 port
內容定址記憶體
412
第二函數轉換器
比對器
來源 IP
413
不符合
封包狀態資料比對
符合
持續進行交握或建立傳輸連線

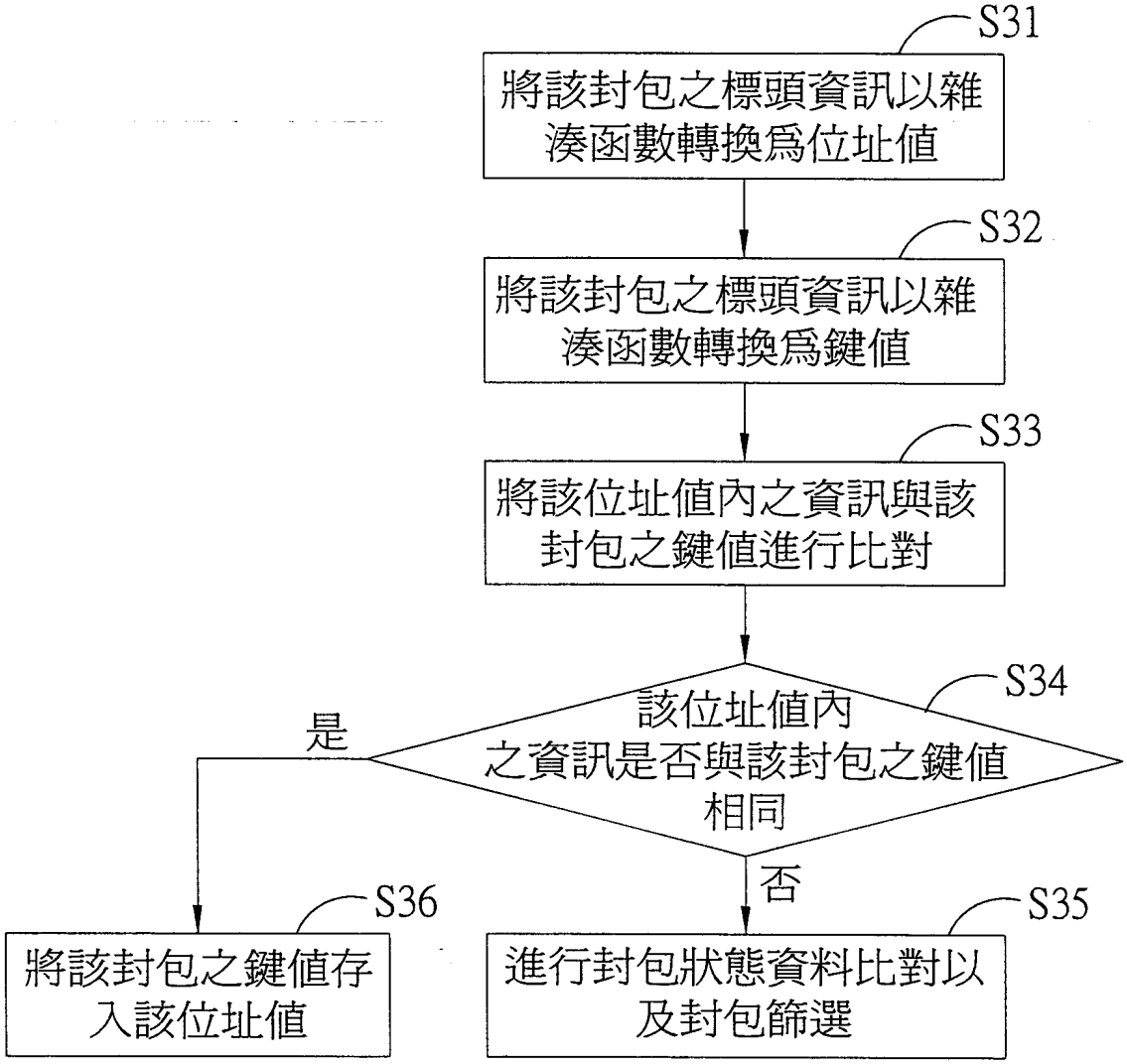
第2A圖



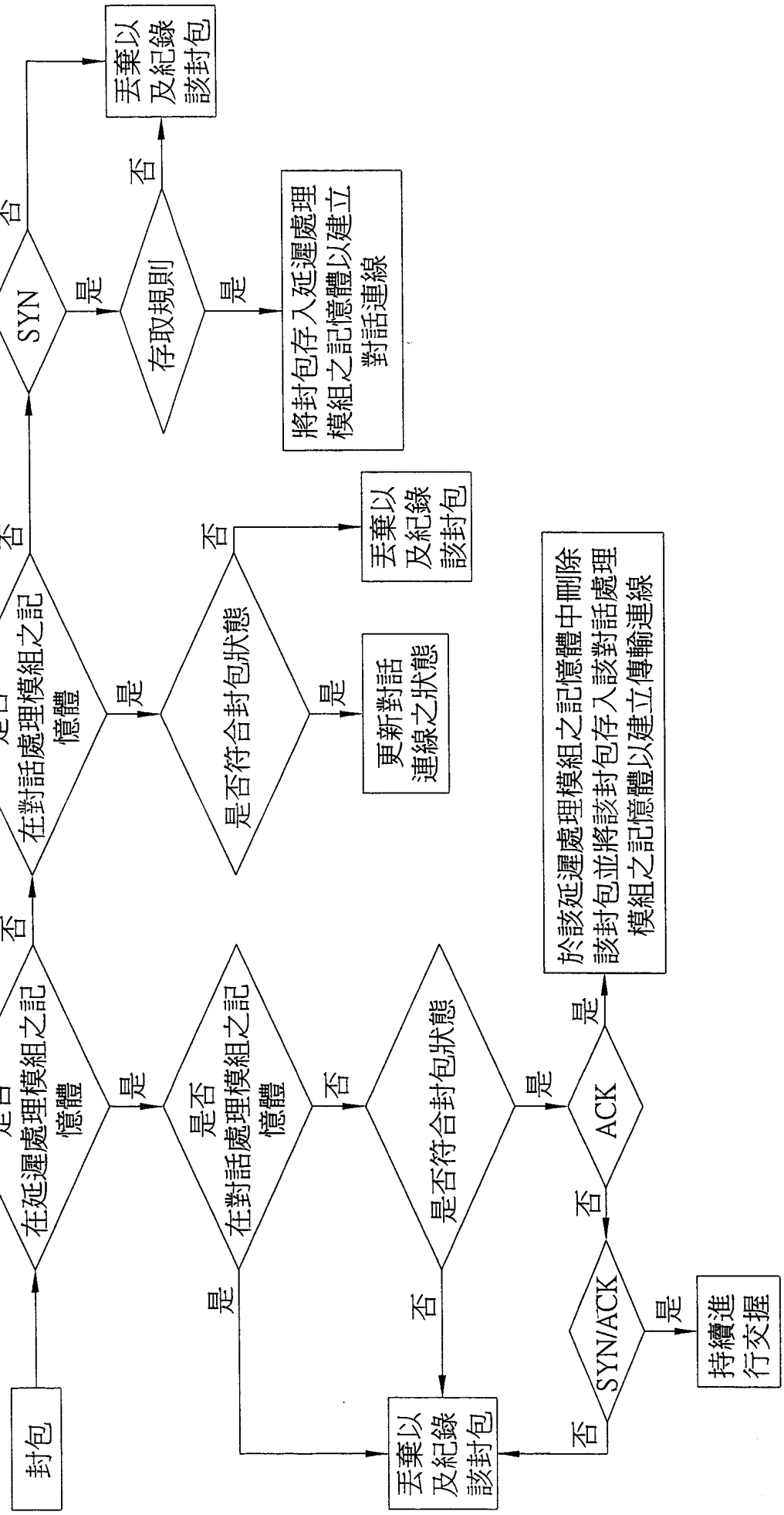
第2B圖


S21
令該延遲處理模組於TCP層交握時透過雜湊函數單元將所接收到封包之標頭資訊轉換爲雜湊函數值並進行比對
S22
記憶體單元中是否具有相同之雜湊函數值
是
否
S23
令該延遲模組建立對話連線
S24
將該封包與對應該封包之對話連線之狀態進行比對
S25
該封包是否符合對應該封包之對話連線之狀態
否
是
S26
令該延遲處理模組持續進行交握或將該封包傳至該對話處理模組以建立傳輸連線
S27
丟棄該封包

第3A圖


S31
將該封包之標頭資訊以雜湊函數轉換爲位址值
S32
將該封包之標頭資訊以雜湊函數轉換爲鍵值
S33
將該位址值內之資訊與該封包之鍵值進行比對
S34
該位址值內之資訊是否與該封包之鍵值相同
是
否
S36
將該封包之鍵值存入該位址值
S35
進行封包狀態資料比對以及封包篩選

第3B圖


封包
是否在延遲處理模組之記憶體
是
否
是否在對話處理模組之記憶體
是
否
是否符合封包狀態
是
否
ACK
是
否
SYN/ACK
是
否
丟棄以及紀錄該封包
持續進行交握
於該延遲處理模組之記憶體中刪除該封包並將該封包存入該對話處理模組之記憶體以建立傳輸連線
是否在對話處理模組之記憶體
是
否
是否符合封包狀態
是
否
丟棄以及紀錄該封包
更新對話連線之狀態
是否在對話處理模組之記憶體
是
否
SYN
是
否
存取規則
是
否
丟棄以及紀錄該封包
將封包存入延遲處理模組之記憶體以建立對話連線

第4圖

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：

1	封包檢測裝置
11	延遲處理模組
111	雜湊函數單元
112	記憶體單元
12	對話處理模組
2	用戶端裝置
3	伺服器

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。