
# 計算機組
# 陳郁堂副教授

美國普渡大學博士
研究領域：資源預留 封包分類策略 密鑰管理
關 鍵 字：封包分類 感測網路
網　　頁：http://homepage.ntust.edu.tw/ytchen
電子郵件：ytchen@et.ntust.edu.tw
電　　話：02-27376420


一、研究主題與目標

我們的研究目標在發展新一代網路技術。包含多媒體網路 、高速骨幹路由器技術 與感測網路的安全機制。

二、最近研究題目

“具彈性之遠程資源預留服務模型”

資源預留（Resource Reservation）為提供具有服務品質（Quality of Service）即時網路的重要方法。資源預留時，可分為 (1)即時預留 與 (2)遠程預留。於遠程預留之研究領域裡，系統資源的最佳化是一個較少被探討之議題。由於系統負荷在不同時段差異性極大，形成在設計遠程預留系統的難題。我們提出一個具彈性的預留模型和資源請求排程之方法來處理這個問題。在預留模型我提出一種具有彈性間隔開始時間的遠程預留。並將此間隔以多階段的有向圖型表示；尋求系統最佳排程問題，可以轉換為在此有向圖型中的尋求最短路徑的問題。利用電腦模擬驗證我們所發展的遠程預留排程的，結果顯示遠程要求之接受率可獲得顯當相著的改善。我們主要貢獻為遠程預留系統最佳化的踏出第一步。

位元重組與層級壓縮在封包分類策略之研究

由於網路處理器興起，運用平行處理技術進行封包分類變為可行。本計劃將封包分類分為法則分割、位元重組、層級壓縮三部份。首先，將封包分類法則，在 prefix length domain 進行分割， 確保同一分割內，分類法則 prefix 長度差異皆在固定範圍。再將同一分割分類法則，交由單一 micro-engine 建立搜尋索引。再利用位元重組(bit selection)技術，對分類法則進行編碼，可有效加速查詢。利用層級壓縮技巧將決策樹層級壓為兩層。不但可加速封包分類器處理速度，也可降低分類法則分布對多欄型封包分類法的干擾。實驗結果顯示，我悶所提方法，在搜尋速度與所需記憶體體積，皆優於現有封包分類演算法，在不利用 pipelining 技術，封包分類演算法，每秒可處理 800 萬封包;所用記憶體也很小，20000 條分類法則，僅需 550K 記憶體。

**平行封包分類演算法中法則切割之探討**

由於網路處理器興起，運用平行處理技術，進行數量龐大分類法則的封包分類變為可行，本計劃針對網路處理器，提出分割式封包分類的設計法。我們從分類法

則分割切入，首先，將封包分類法則分為一維法則與二維法則，並將一維法則交由 Longest Prefix Match 演算法執行。為確保有效降低儲存空間，則進一步發展 modified ***K-means*** 演算法，對於二維法則在 tuple space 進行分割，***K-means*** 演算法中距離函數的發展為本研究的關鍵。為驗證法則分割式平行封包分類法的系統效能，我們利用電腦模擬進行測試，結果顯示，在二十萬條法則中，有百分之八十六的一維法則下，我們所提分割式封包分類法，即使在最差情況，仍可達每秒一千三百萬次封包分類，而且所需記憶體也僅 4.8MB，優於現存其他的封包分類方法。

**分散式感測網路上前置密鑰之研究**

在分散式感測網路(Distributed Sensor Networks)中，受限於資源限制，金鑰管理(key management)變成一個重要的新課題。礙於有限電源供應及儲存裝置，公開金鑰加密或置入所有的密鑰對，並不適用於感測網路。最近，隨機式前置金鑰分配(probabilistic key pre-distribution)被認為是可行的方式，感測器從一個極大的密鑰池(key pool)內，隨機選出部份密鑰做為其金鑰環(key ring)，當佈署於環境的同時，藉由部份的密鑰與鄰近的節點做安全性溝通。當感測網路遭受攻擊時，不安全的密鑰必須移除。我們藉由數學分析及實驗分析，發現在 5%的節點遭受攻擊後，分散式感測網路的安全機置已經失去效用。然而以往隨機式前置金鑰分配的相關研究，無法針對此問題提供有效解決方案。本計畫將發展一個蛇型前置密鑰演算法(snake　key pre-distribution)，有效的來解決這個問題。感測器從一個二維的密鑰表(two-dimensional key table)，以蛇型方式選出部份密鑰，藉由密鑰在二維空間的相依性，我們能正確且快速的對系統所發出的新密鑰進行解密。即使密鑰池的數量級達到數萬，我們仍可控制感測器解密的複雜度在 $O(1)$；我們並利用感測器散佈的相關資訊，降低儲存裝置需求。

三、主要的研究成果與所執行的計劃

(一) 論文

[1] Yie-Tarng Chen and Kai-Hui Lee “A Flexible Service Model for Advance Reservation.” Computer Networks (SCI), Vol. 37, pp.251-262, 2001

[2] Yie-Tarng Chen and Shin-Shian Lee “An Efficient Packet Classification Algorithm for Network Processors"　IEEE International Conference on Communications (ICC 2003), Anchorage, Alaska, USA on May 11-15, 2003

(二) 計畫

1. NSC94-2213-E-011-059 分散式感測網路上前置密鑰之研究
2. NSC93-2213-E-011-073 平行封包分類演算法中法則切割之探討