第一章　緒論

第一節　研究背景與動機

近年來由於無線網路的方便及其行動性，使得無線網路快速發展，IEEE 於 1999 年起相繼推出 802.11、802.11a、802.11b、802.11g 等標準，802.11 無線區域網路標準(wireless local area networks)因此誕生，網路傳輸效能上的問題，也是企業關心的議題，如何在固定時間內傳輸最多的資料，或如何使傳輸速率更快都是重要的議題，當網路上的應用越來越多時，流量的負載也會越來越重，在效能上也產生影響。在另一方面，無線網路有著較有線網路較弱的安全性，且近年來網路駭客及各種病毒猖獗，如何使無線網路的安全性提升，是大家注重的課題，IEEE 802.11 的各種安全機制便不斷出現，如 WEP、WPA 等。由於安全機制的不斷加強，如加解密、驗證等會導致效能上的損失，因此本研究即為討論安全機制對無線網路的效能上的影響。

第二節　研究目的

本研究利用網路擷取封包軟體 Wireshark 擷取封包，分析無線網路安全機制對效能的影響，在 802.11g 的環境中使用四種安全機制：WEP 64 位元、WEP 128 位元、具 WEP128 位元之 802.1X、WPA 及兩種評估參數：流通量與反應時間，來說明它們對效能的影響：

一、四個安全機制對網路流通量的影響。

二、各安全機制對TCP/UDP訊務效能的影響之差異。

三、各安全機制對802.11b與802.11g網路效能影響的差異。

四、各安全機制對客戶端(client)多寡在效能上影響的差異。

五、各安全機制對不同packet size在效能上影響的差異。

第三節 研究步驟

一、資料蒐集與文獻

蒐集關於無線網路設備的支援性資訊，以及蒐集關於無線區域網路協定、無線區域網路安全機制、網路效能的文獻，參考國內外相關的期刊論文以及目前網路上可以提供上的資源，作為本研究的構想。

二、實驗驗證法

考慮可能影響網路效能的參數，並開始實驗其影響的程度且加以分析，且測試 NO-WEP、WEP 64 位元(wired equivalent privacy)、WEP 128 位元、具 WEP128 位元之 802.1X、WPA (Wi-Fi protected access)等無線區域網路安全機制影響其網路效能的分析，接著加入各參數在安全機制下對效能的影響，像封包的長度、 TCP/UDP 或 client 的數目等。

以下為本研究的步驟流程圖，如圖 1-1

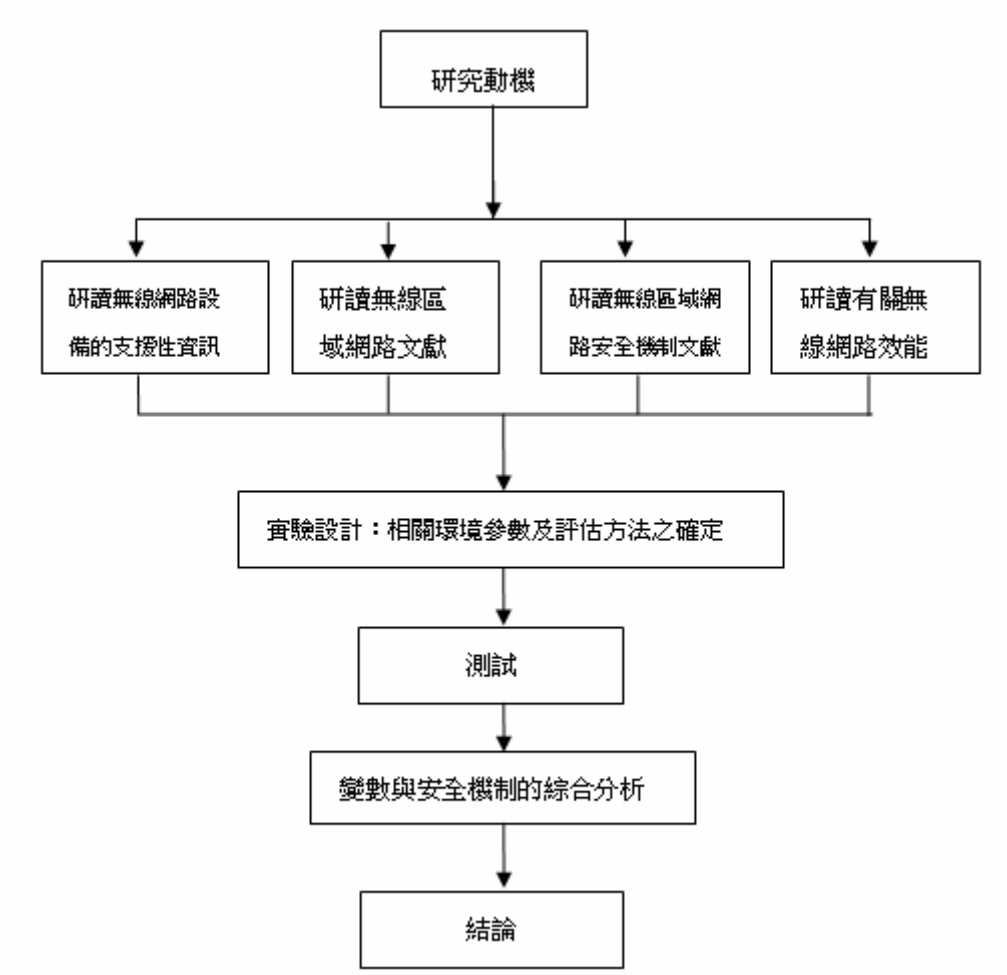

圖 1-1　研究流程圖

第四節　研究範圍與限制

本研究的主要研究範圍是 802.11g、802.11b 網路下運作的四種安全機制(WEP 64 位元、WEP 128 位元、具 WEP128 位元之 802.1X、WPA)。以下是本研究的限制：

一、因為設備不足，不考慮 ESS (extended service set)及 802.11i、802.11n。

二、安全機制上並沒有包括 WPA-PSK(因為它是 WPA 的簡化版)以及 EAP (extension authentication protocol)中除了 EAP-TLS 外的其它驗證方法，因為它提供了相對於其它 EAP 方法更為安全的驗證方式。

三、本實驗處在一個封閉的小型實驗環境中，存取點、客戶端及 Radius server 距離皆未超過 1.5 公尺，而倘若 Radius server 在外地的情況下，於本實驗並不適用。