計畫名稱：適用於物聯網之數位鑑識與分析雲端平台
子計畫三 - 匿蹤犯罪網路源點鑑識

執行單位：中原大學大學/資訊工程學系
主持人：　楊明豪教授

計畫編號：MOST 106-2221-E-033-002

計　畫　摘　要

網路已與我們的生活密不可分，而近年各種網路攻擊事件層出不窮。攻擊者常以阻斷服務攻擊，來擾亂伺服器的服務。諸多犯罪藉由各式匿蹤技術，令網路犯罪的查緝非常困難。為追溯軟體弱點攻擊之來源，我們於本次計畫實作一個：零路由器儲存需求的單一封包網路匿名犯罪源頭鑑識方法。本計畫所提出之方法將有以下能力：單一封包網路匿名犯罪源頭鑑識、路由器零儲存負擔、零漏判率和低誤判率。

技　術　特　色

- 攻擊路徑記錄於IP表頭
- 只需要32bits進行標記
- 能夠辨別偽造來源的網路攻擊
- 單一封包源頭鑑識
- 路由器零儲存負擔
- 零漏判率
- 低誤判率

計　畫　架　構

技　術　應　用　範　圍

- 結合IDS/IPS/防火牆，使其能準確地找到並過濾攻擊流量。
- 和無線定位技術結合，定位攻擊者的實際位置。