

物聯網之繞路協定的入侵偵測模擬與研究

系所／資訊工程學系

指導老師／蘇民陽

組員／徐王迪、謝承宇、陳銘庭

移動通訊和能夠通過遠程連接進行控制的物聯網產品現在越來越成為千家萬戶擁有的事。但是因為現在的物聯網防入侵技術的限制加上對於這樣一個新型出現的東西沒有具體的管控措施，會讓有些不法駭客利用物聯網的漏洞進行攻擊，例如駭客入侵學校的印表機對其資料進行篡改造成大面積的損失，家中的攝像設施被監視然而使用者並不知情。我們小組針對 6LoWPAN 網路上的 RPL (Routing Protocol for Low-Power and Lossy Networks) 繞路協定的攻擊，例如 Selective Forwarding Attack，做分析探討，並用 cooja 模擬器對物聯網裡存在的駭客入侵進行模擬分析。

本專題目的即是利用 cooja 的軟體類比物聯網中針對繞路協定的入侵偵測找出存在物聯網中的入侵。

目前專題成果如圖 1、圖 2 所示。圖 1 為 cooja 系統的顯示介面，可由左上角選項打開一個攻擊模擬的結果，點擊一個打開後可以至圖 2 的類比畫面。在畫面內可以移動，修改各個點之間的

距離。上方列則可打開各個指標值來進行查看，比如點之間的訊號傳輸過程，每個點的資訊。每個點都可以根據收集的資料來查看電量的消耗程度，然後各個點之間的資訊交換內容。我們先對節點個數進行設定，然後再將其中一點設為攻擊者，在封包不斷地交換過程中獲取適當的資料進行分析，發現攻擊節點的攻擊方式，用於總結。

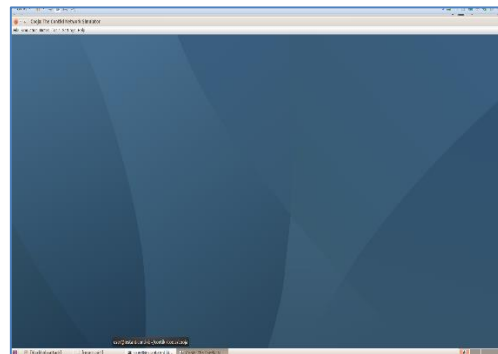


圖 1：cooja 模擬系統登入畫面

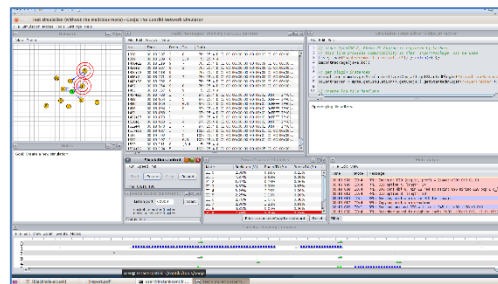


圖 2：cooja 模擬系統運行畫面