計畫名稱：雲端服務之整體資安防禦系統—
一個基於Fed-MR的通用型協同式P2P殭屍網路偵測系統

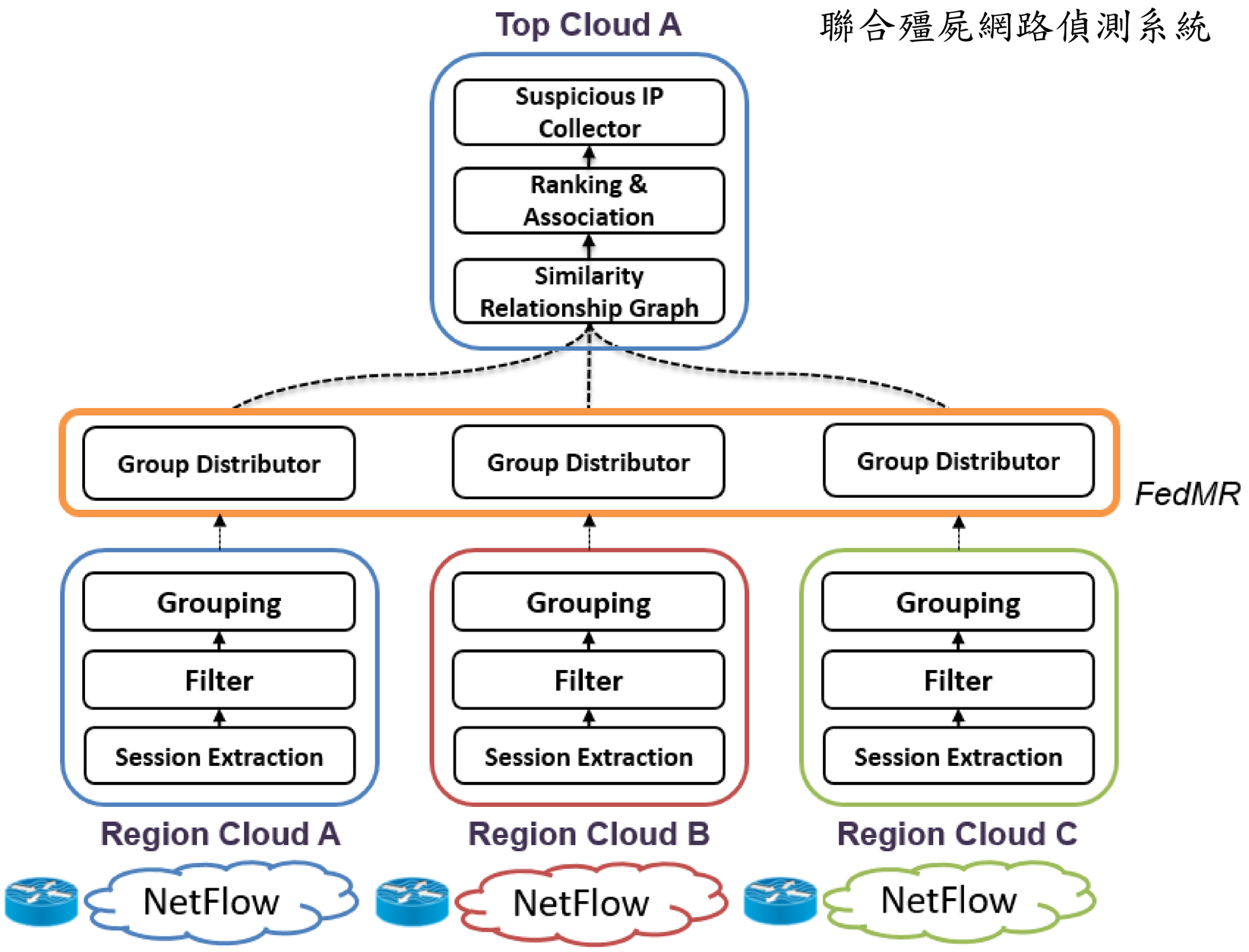
執行單位：國立成功大學電機工程學系（所）
主持人：謝錫堃老師、張志標老師

計畫編號：MOST 103-2221-E-006-144-MY3

一、計畫摘要

本計畫提出一個通用型P2P殭屍協同式網路偵測平台，以解析相同網路行為概念設計能夠偵測出不同種類的P2P殭屍網路活動，並可應用於未來防禦新型P2P殭屍網路攻擊。透過協同式運算平台執行跨區運算，交互分析不同區域的網路流量日誌，以達成跨區域聯合防禦的目標。此外本計畫也建構跨區域分散式檔案系統，可用於存放網路流量日誌資料庫，並對提供巨量資料規模的網路流量日誌進行快速存取及運算。本計畫預計將該偵測系統佈署至學術網路，提供一套完善的資安偵防機制，以期協助P2P殭屍網路行為偵測，消弭資安威脅。

二、計畫架構



三、技術特色

- 通用型P2P殭屍網路偵測演算法
  1. 能偵測P2P殭屍網路在潛伏階段的微量通訊行為，在殭屍網路發動攻擊前就將有嫌疑的流量及來源IP偵測出來
  2. 不需對封包內容進行分析，確保個人隱私以及避免加密技術的問題
- Federated MapReduce 跨區域聯合運算

  基於Hadoop系統修改的架構，可聯合多個叢集進行運算，並優化遞迴運算時資料重複傳遞所造成的額外開銷，提升運算效率以及減少資源浪費

四、技術應用範圍

與目前透過特徵值(signature-based)來偵測P2P殭屍網路病毒的系統比較，本系統的優勢在於不需要建立特徵值資料庫做比對。

本計畫可應用於學術網路(TANet)，收集學網的網路流量分析其中有哪些主機感染了殭屍網路病毒，另外也可應用於HiNet等電信業者提供更進一步的資訊安全服務。

Prof. Ce-Kuen Shieh
Institute of Computer and Communication Engineering
National Cheng Kung University