經濟部 111 年度

《5G 資安防護系統開發計畫》

合作研究計畫

5G智能惡意流量防禦技術

建議書徵求文件

財團法人資訊工業策進會

中華民國111年01月28日

111年度合作研究計畫建議書徵求文件

一、 簡介(說明本合作研究計畫之背景、動機、目的及重要性)

隨著5G網路和IoT時代到來，網路使用量遽增，駭客的攻擊活動數量也逐年上升。在5G網路下有許多應用服務伺服器每天需提供大量連線服務，在效能緊繃的情況下，如果受到駭客DDoS攻擊，將會造成許多服務中斷。在未來電動自駕車普及時，將相當仰賴5G網路，因DDoS攻擊而造成的效能影響可能會導致車禍甚至人員傷亡。

DDoS攻擊種類眾多，包含了在IP Layer攻擊之ICMP Flood，在TCP Layer攻擊之SYN Flood、ACK Flood、 ACK PUSH Flood等，以及在Application Layer攻擊的DNS Amplification、HTTP Flood等，不同的攻擊手法需要仰賴不同的防禦手法，其中Application Layer的攻擊最容易透過少量攻擊資源而造成服務伺服器的癱瘓，但貿然中斷使用者的應用服務連線可能會使服務不完整造成使用者和服務供應上金錢上之損失，因此在面臨此攻擊時應比其他DDoS攻擊更加謹慎處理。

二、 計畫目標(應包含本合作研究計畫預期可達成或量化的目標)

本計畫目標為開發結合區塊鏈中PoW(Proof of Work)和AI技術以減緩DDoS於Application Layer的攻擊，建構出智能惡意流量防禦技術，架設於應用伺服器之前端，保障該應用伺服器的網路的安全和順暢性。

三、 計畫範圍(說明本合作研究計畫所需執行之項目)

本計畫範圍為研究工作量證明PoW機制如何應用於使用者端，透過PoW機制控制使用者對於應用伺服器的負擔(Load Balance)，以及透過收集過去使用者的連線技術和身分指紋搭配人工智慧技術進行學習，打造可自適應調整的存取管控(Access Control)模型，用此減少惡意使用者對應用伺服器發出的DDoS攻擊。

四、 預期成果(說明在執行期限內應完成之工作項目/成果及交付時程)

- 期中研究報告一份，內容包含：系統架構的規劃方式及先前技術整理說明，包含PoW、AI技術、DDoS防禦等相關文獻探討。
- 期末研究報告一份，內容包含：系統操作行為檢測模組的研究成果、相關的功能驗證報告、驗證測試資料集及雛形展示，包含測試應用服務在有無防護系統下的效能影響。
- 雛形系統原始碼一份：包含軟體模擬之可部署於應用伺服器的智能惡意流量防禦技術、減緩DDoS攻擊之PoW機制和訓練之AI模型。
- 提供教育訓練：針對計畫成果移交、系統運作機制及操作說明等提供教育訓練。

- 進度討論會議：每月召開線上或實體會議。
- 國內外知名研討會或期刊論文投稿一篇。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後6個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、 執行方式(包括計畫時程、計畫分工方式、執行事項，但不限於前述項目)

- 合作計畫執行單位應配合本會計畫監控機制。
- 於計畫執行期間，合作計畫執行單位須配合計畫所需，不定期與本單位進行研究心得報告與研討，報告內容以計畫範圍相關之技術主題為主。
- 交付說明

項次	交付項目	交付內容	數量	交付型態	交付期限
1	期中研究報告一份	• 系統架構的規劃方式 • 先前技術整理說明	1 份	電子檔	111 年 8 月 31 日
2	期末研究報告一份	• 系統模組的研究成果 • 相關的功能驗證報告 • 驗證測試資料集 • 雛形展示	1 件	電子檔	111 年 11 月 30 日
3	智慧縱深代理伺服器系統一式	• 原始程式碼，含使用安裝說明 • 包含軟體模擬之可部署於應用伺服器的智能惡意流量防禦技術、減緩 DDoS 攻擊之 PoW 機制和訓練之 AI 模型。	1 式	電子檔	111 年 11 月 30 日
4	投稿國內外知名研討會或期刊論文一篇	• 投稿論文證明	1 份	電子檔	111 年 12 月 15 日

六、 計畫期程及預估計畫總經費

計畫執行區間：111年01月01日至111年12月31日

總經費：1,200,000元

七、 驗收標準(含教育訓練)

- 依本建議書徵求文件第四章「預期成果」規定，如期繳交相關成果。

八、 技術能力需求(請詳述所需要之技術能力或專長)

本計畫執行人員須具備電信網路研究背景外，尚須對網路安全、網路流量分析和網路系統性能評估擁有相關經驗背景。

- 具行動通訊網路研究經驗之學界研究人員
- 具備且熟悉無線網路與TCP/IP協定技術之學界研究人員
- 具備5年以上資安研究經驗
- 發表超過3篇以上與資安相關的國際期刊或會議論文