經濟部111 年度

《5G 資安防護系統開發計畫》

合作研究計畫

5G協定攻擊威脅技術

建議書徵求文件

財團法人資訊工業策進會

中華民國 111 年 03 月 01 日

111年度合作研究計畫建議書徵求文件

一、簡介

未來第五代行動通訊（5G）技術最多的應用將不只是提供給民眾上網使用，而是在商用環境中讓許多的設備，如 IoT 裝置連線，並利用 5G 的三個場域：增強型行動寬頻（enhanced mobile broadband; eMBB)、極低延遲的可靠通訊(ultra-reliable and low latency communications; uRLLC)以及巨量物聯網通訊（massive machine type communications; mMTC)，提升用戶及裝置的使用體驗。而 5G Stand Alone （SA）架構更是 5G 的最完整形式，也是工/商業中將使用的場域。本計劃為因應將來 5G SA 的發展趨勢，需設計一針對 SA 環境的協定攻擊偵測及完整性檢測的邊緣運算（Multi-access Edge Computing; MEC）元件，該元件需在不修改電信商的核心網路前提下進行檢測。如前述5G SA 將更廣泛的應用在工/商業中，如遠程醫療、運輸安全及智慧工廠等情境中，此時若 RAN 端遭駭發出協定攻擊，或是本身設計不良發送未完整加密的資訊，將對上述場景造成嚴重的影響，因此 MEC 須在 RAN端的 gNB 及 5GC-AMF 間擔任檢測的工作，必要時能保護核心網路，並警示相關人員。

二、計畫目標

檢測gNodeB傳送的所有信令，但要在不能修改電信商的核心網路狀況下進行監測。現今的邊緣運算技術MEC不斷地發展起來，透過MEC將信令進行監聽檢測為未來趨勢。我們將計畫分成三個議題，基於這三個議題才能進一步實現5G SA異常信令檢測及安全性檢測。

議題一：建置完整的 5G SA 並且結合 MEC

因實驗初期不能直接對接真實電信網路環境，因此必須要自行建置一 5G SA 環境，同時也可以於封包處理上。建置完成之後，需建置一邊緣運算節點(Multi-access Edge Computing; MEC)串接至 RAN 端與 AMF 之間，並且 MEC 要能夠解讀 NGAP 上的所有信令。

議題二：建置 RAN 端發起異常信令，並對核心網路之行為進行測試

當 RAN 端發起異常信令，需檢測是否對於 AMF 造成威脅，並需透過 MEC 檢測是否為惡意終端設備發起的攻擊。

議題三：MEC 之資安檢測機制

由於 MEC 可以針對所有流經的流量進行截取處理，因此 MEC 須有判

斷是否有信令交錯或者惡意封包等等資訊的能力。若能判斷出惡意資料流時，需針對惡意流量進行處理，以確保安全性。

三、 計畫範圍

本計畫範圍以建構 5G SA實驗環境平台，並於平台中於gNB產生異常信令，並針對其進行檢測，主要研究範圍如下:

1. 產生gNB異常信令，包含「NAS-PDU Security header type」、「不完善的加密如EIA0」類型。
2. 探討異常信令攻擊設計及實作，完成1篇報告，並完成 1 篇國外會議論文投稿。
3. 研究具安全檢測機制的MEC並完成 1 篇國外會議論文投稿。

四、 預期成果

- 期中報告一份，預計於 111 年 8 月 31 日完成交付。

  內容：系統架構的規劃方式及先前技術整理說明，包含以下項目：

  - 建置可提供完整 5G SA 網路環境之場域。
  - 研究彙集 5G SA 信令及核心網路 AMF 和基地台 gNB 之溝通過程。
  - 建立邊緣運算節點且具檢測流量之 MEC 元件。

- 期末報告一份，預計於 111 年 11 月 30 日完成交付。

  內容：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，包含以下項目：

  - 設計異常信令攻擊，內容包含：設計 RAN 端發起異常信令、設計異常演算法達成沒有完整性保護。
  - 實作具檢測 NAS-PDU 異常信令之 MEC 元件。gNB 提供連線服務時， MEC 可以檢測出 gNB 其 NAS-PDU 信令是否符合 3GPP TR 33.809、TR 33.853 規範。
  - 實作具檢測沒有完整性保護及未加密演算法的信令之 MEC 元件。MEC 可以檢測出核心網路提供之加密演算法及完整性保護是否符合 3GPP TR 33.809、TR 33.853 規範。

- 雛形系統原始碼一份：包含 5G SA 環境與攻擊、檢測模組雛形原始程式碼，與使用安裝說明、系統功能摘要。
- 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 2 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

●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，每月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1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1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 ●教育訓練	1 件	電子檔	111 年 11 月 30 日
3	5G協定攻擊威脅技術系統1式	●原始程式碼，含使用安裝說明 ●系統功能摘要	1 式	電子檔	111 年 11 月 30 日
4	國內外知名研討會或期刊論文 2 篇	●論文 2 篇 ●投稿論文證明 2 式	1 份	電子檔	111 年 12 月 07 日

六、 計畫期程及預估計畫總經費

計畫執行區間： 111 年 03 月 01 日 至 111 年 12 月 15日

總經費：800,000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

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
- 國內外知名研討會或期刊論文 2 篇