透過部屬安全邊緣防護代理以增強5G漫遊之安全性
Implement Security Edge Protection Proxy (SEPP) to enhance 5G roaming security

國立陽明交通大學 資電亥客與安全碩士學位學程
研究生：楊惟鈞 指導老師：陳志成

摘要

隨著行動網路從1G演變到現今的5G，行動網路所提供的功能越來越多，而第五代行動網路(5G Cellular Networks)則是跳脫了以往服務一般手機用戶為主，開始提供各項垂直服務應用，如智慧工廠、智慧城市等類型，且這些服務會使用大量須連上網路才能使用的裝置。因此使用行動網路的對象大幅增加，也導致行動網路面臨龐大的數據壓力與傳輸延遲的問題。除此之外，內部資訊的安全性對於智慧工廠來說也是非常重要的。5G專網能夠藉由5G速度快、延遲低、頻寬大的特性，提供擁有高安全性的高品質專網服務，且專網於企業內網傳輸進行，不經過公網，所以可以確保資料安全及避免機密資訊外流，提升企業內部效能。而為了讓各個專網能夠與彼此及公網之間溝通以支援漫遊服務，就需要Security Edge Protection Proxy(SEPP)來確保資訊的安全。

本篇論文針對不同核網之間的控制端(control plane)訊息交換，實作出符合3GPP制定之規格的SEPP以及位於不同核網之間的N32 Interface，並利用本實驗室所實作的5G開源核心網路free5GC來進行測試。

最後針對N32 Interface在採用不同安全機制下的通訊延遲來作比較，並驗證資訊的正確性。

方法

SEPP(Security and Edge Protection Proxy)為5G網路中主要負責跨核網之間溝通及加密的重要網路功能，兩個SEPP中間溝通的Interface是N32，而N32所採用的Protocol為HTTP/2 protocol。

SEPP跟任意NF之間的TLS保護主要有基於TLS萬用字元憑證和生成Telescopic FQDN之方法，或使用3GPP所制定的客製HTTP Header(3gpp-Sbi-Target-apiRoot)方法。

基於free5gc之實作機制本論文實作之SEPP選擇採用3GPP所制定的HTTP Header。

3GPP選擇使用JWT來對N32-f interface的訊息作保護

結論

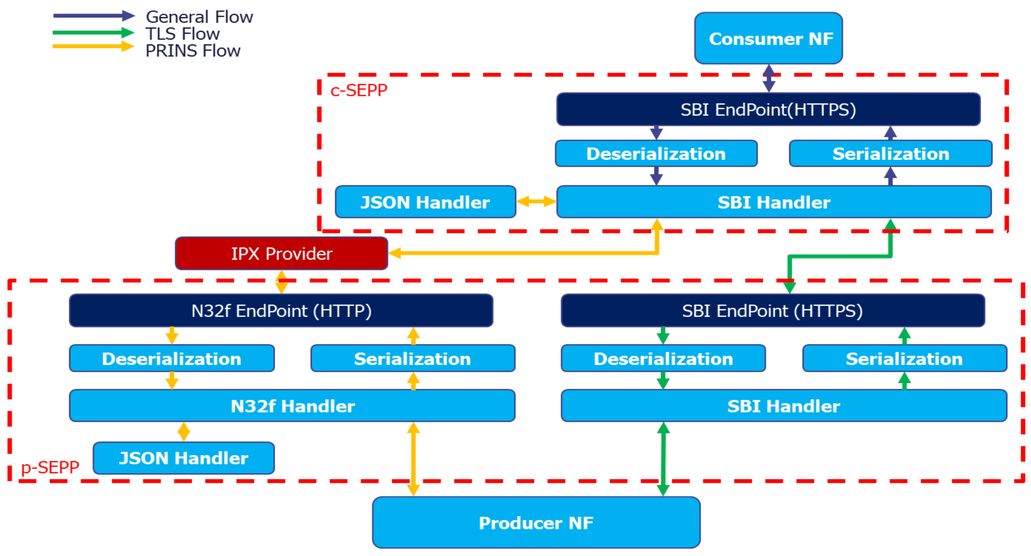
在本篇論文中，介紹了5G核心網路之間溝通的架構，並根據3GPP Release 16中的N32 Interface概念設計SEPP並實作TLS與PRINS兩種安全機制出來，使得核心網路之間可以進行溝通。

經實驗得出結果表明採用TLS作為安全機制時對於延遲時間的影響不大；而當採用PRINS時，因為必須對應用層的資料作加解密，所以造成延遲時間大幅增加，同時也透過與free5GC對接進行測試，驗證了此SEPP的可行性，因此開發者們可以放心使用此SEPP。

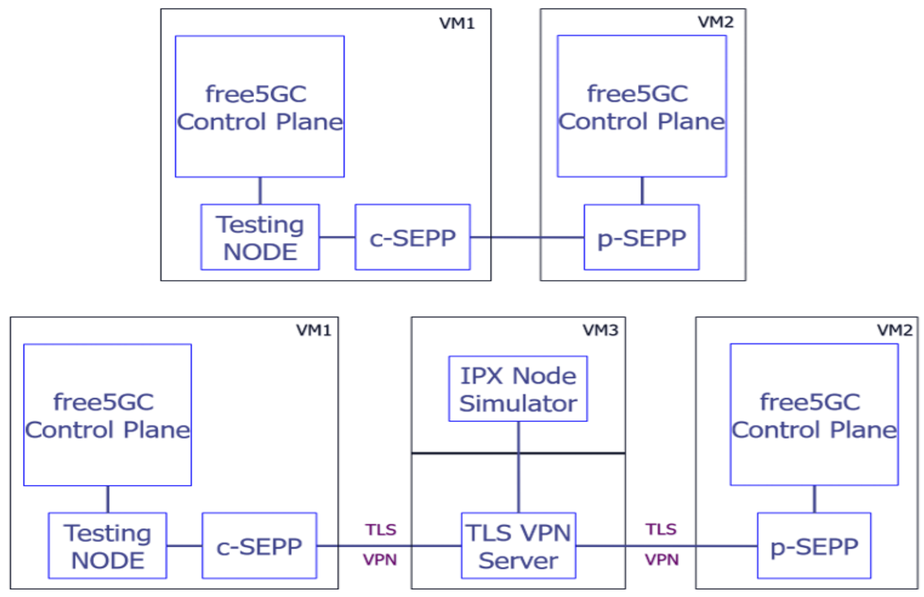
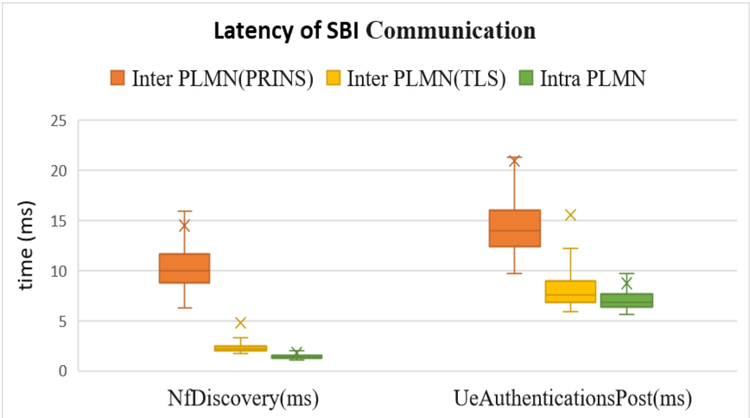
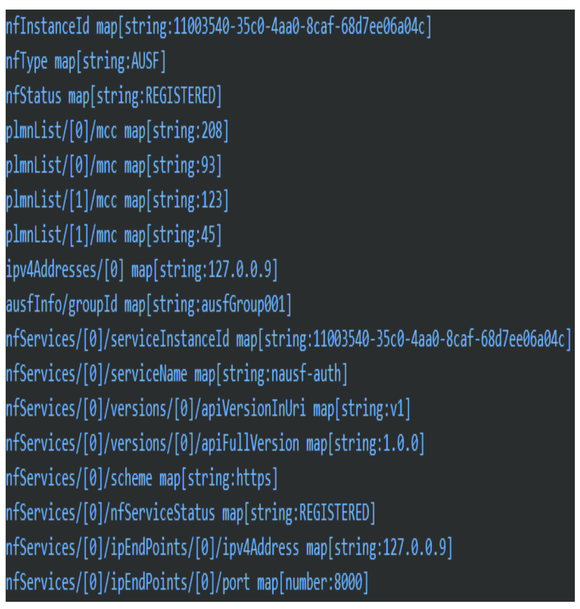
採用TLS為安全機制的優點是不會對延遲時間產生太大的影響，但當有大量且複雜的漫遊關係時不建議使用

PRINS的優點是當有大量且複雜的漫遊關係時，IPX服務商會協助處理，但缺點是為了確保點對點加密的特性而會造成大量的延遲。

系統架構



實驗架構



實驗結果