4G LTE 企業專網中惡意基地台攻擊偵測與通知

洪稟凱[1*]、何筱珊[1]、林裕翔[1]、黃俊鴻[1]、鄭欣明[12]
[1]國立臺灣科技大學資訊工程學系、[2]中央研究院資訊科技創新研究中心
{d10815003, m10815009, m10915204, m10915007, smcheng}@mail.ntust.edu.tw

摘要

近年來，由於低成本軟體定義無線電 (Software-Defined Radio, SDR) 興起，利用訊號強度吸引手機或 IoT 設備並且傳送 4G 惡意信令的惡意基地台攻擊行為日漸增加，偵測這些未經授權的惡意基地台就愈加重要。在本文中，我們旨在利用惡意基地台的不穩定信號強度與接取邊緣運算節點 (Multi-access Edge Computing, MEC) 的幫助來提高偵測 4G 惡意信令攻擊企業專網 (Non-public network, NPN) 的準確性，我們也設計了通知的機制來讓有註冊的使用者可以得知惡意基地台攻擊的發生。我們採用基於 NAS 層漏洞的 Attach Reject 攻擊當作偵測對象。此外，我們使用開源軟體 srsRAN 和低成本的 SDR 建構可發送惡意 Attach Reject 訊息的 4G 惡意基地台。在企業專網環境中利用 srsUE 和商用 SIM 卡結合 SDR 設計一個可接收來自合法和惡意基地台信令的偵測器。該偵測器可以接收來自合法和惡意基地台的信令並運行我們提出的偵測機制，而偵測器將佈置於企業專網環境中的各處，偵測機制的流程是利用惡意基地台發送的 PHY 層參考信號接收功率 (Reference Signal Received Power, RSRP) 的不穩定特性，計算 SIB1 和 Attach Reject 之間的最大訊號強度差來區分收到的訊息來自合法或惡意基地台，最後分散在各處的偵測器會將訊息回傳到多 MEC 上，而 MEC 也會將判定結果知會有註冊此服務的使用者，而讓使用者知道惡意基地台的存在。實驗結果表明，使用 RSRP 區分 Attach Reject 訊息的準確率為 91%。

關鍵詞：4G LTE、多接取邊緣運算節點、專網、惡意基地台攻擊、惡意基地台偵測、軟體定義無線電

Regular Paper

Communications of the CCISA
Vol. 27 No. 4 Nov. 2021

Detection and Notification of Rogue BS Attack in 4G LTE Non-Public Networks

Bing-Kai Hong[1*], Siao-Shan He[1], Yu-Xiang Lin[1], Jun-Hong Huang[1], Shin-Ming Cheng[1, 2],
[1]National Taiwan University of Science and Technology,
[2]Research Center for Information Technology Innovation
[1]{d10815003, m10815009, m10915204, m10915007, smcheng}@mail.ntust.edu.tw

Abstract

Recently, the rise of low-cost Software-Defined Radio (SDR) increases the possibility of rogue BS attacks, where UE and IoT devices are attracted to connect the rogue BS and perform actions instructed by the rouge BS. The detection of such unauthorized BS becomes a critical issue. In this paper, we utilize the unstable signal strength from such low-cost BS and the aid of Multi-access Edge Computing (MEC) to increase the detection accuracy of rouge BS attacks in Non-Public Network (NPN). In particular, we apply Attach Reject attack in NAS layer as detection target. Moreover, we use open-source software srsRAN and low-cost SDR to construct 4G rogue BS, which could send malicious Attack Reject message. We exploit srsUE and commercial SIM to build a sensor who could receive signals from rogue and legal BSs and deploy the sensor inside NPN. We investigate unstable property of Reference Signal Received Power (RSRP) of signal sent from rogue BS and calculate the maximum strength difference between SIB 1 and Attach Reject message to determine the rogue BS. The detection results are collected in MEC to increase detection accuracy and further notified to the subscribers so that users are aware of the existence of rogue BS. The experimental results show that the detection accuracy could reach 91%, which validates the feasibility of the proposed mechanism.

Keywords: 4G LTE, MEC, Non-Public Networks, Rogue BS Attack, Rogue BS Detection, Software Define Radio

壹、前言

隨著通訊技術的進步，第四代 4G 長期演進 (Long Term Evolution, LTE) 使人們能夠藉由異構的移動設備隨時隨地存取通訊網路，並且企業專網的理念也漸漸浮出，電信網路已經成為民眾生活中不可或缺的基本服務，而其安全性也會直接影響到使用者的人身安全。近年來軟體定義無線電 (Software Defined Radio, SDR) 技術的出現，使學者可以透過便宜的價格架設 4G LTE 的實驗環境，而攻擊者能透過 SDR 架設低成本的惡意基地台，並利用 LTE 協議中的漏洞進行各種攻擊 [21]。例如：使用惡意基地台發送干擾信號，迫使附近設備的網路降級 [4]；發送垃圾郵件 [20] 和緊急警報 [16], [32]或者攻擊者也可以利用惡意基地台監控國際移動使用者辨識碼 (International Mobile Subscriber Identity, IMSI) 以跟踪用戶行為 [12]。而企業專網的興起，讓低運算量的專網內具 4G 通訊能力的物聯網設備成為一個很好的攻擊對象，為了大幅減少惡意基地台造成的負面後果，偵測惡意基地台變成企業專網中一個重要的資安議題。

目前已有許多偵測惡意基地台的研究，根據進行偵測的位置分成三類。第一個是基於設備的偵測器 [1], [3], [8],[33]，透過在物聯網設備或移動電話運行自行設計的應用程式來收集數據以進行偵測。第二種是基於網路的偵測器 [22], [30]，直接在營運商控制的移動網路中進行分析和偵測。第三種是基於伺服器的偵測器 [2], [20], [23], [25]，藉由移動設備或感測器收集數據，再將數據轉發到伺服器進行偵測。

然而當我們分析上述機制用於偵測惡意基地台的可行性時，發現大多偵測方法都使用當下的 PHY 層參考信號接收功率 (Reference Signal Received Power, RSRP) 來進行偵測，因攻擊者都使用低成本的軟體無線電設備建設惡意基地台，使得訊號強度相較於合法基地台更加不穩定。但我們認為僅使用信號強度的大小或範圍來識別容易產生誤判，又因 RRC 層的訊息皆採用明文傳送，極容易被偽造，因此亦不能有效用來偵測惡意基地台。Phoenix [8] 藉由分析接收到的 NAS 訊息之順序是否符合標準程序，其被認為是一個有效的可以偵測惡意攻擊的方式。但在某些場景下 Phoenix 的偵測不夠全面。例如：Phoneix 收到 Attach Reject、Tracking Area Update (TAU) Reject 或 Service Reject 訊息時，會直接判斷為惡意攻擊，原因是這類 Reject 訊息在現實中並不常見，但在 LTE 規範中仍然存在，所以 Phoenix 僅藉由接收到的 Reject 訊息進行判斷容易造成誤判。

若只使用一種 PHY、RRC 或 NAS 層的資訊作為識別的依據，容易出現上述各種誤判情況。在本文中，為了提高 4G LTE 中惡意基地台攻擊企業專網 (Non-Public Networks, NPN) 偵測的準確性，我們使用開源軟體 srsRAN 的 srsUE 設計一個基於設備的偵測器，我們也建立了一個企業專網當作實驗環境，我們在專網當中建立了一個多接取邊緣運算節點 (Multi-access Edge Computing, MEC)，其與偵測器互相合作來判斷惡意基地台的存在，並且我們開發了一個由 MEC 主導的在地化應用程式與相對的 APP 服務。偵測器會不斷搜集附近基地台的信令資訊，並且分析此資訊的行為模式與穩定度，並且將判斷為可能有惡意的相關資訊傳輸給 MEC。而 MEC 透過搜集多個偵測器的回應

來判斷惡意基地台的存在，並且將判斷結果通知給有註冊此服務的用戶 APP 上。

在實驗中，我們實作了在 NAS 層透過發送 Attach Reject 而達到的 DoS 攻擊，當作我們的偵測機制判斷的目標。實驗結果表明，在接收 Attach Reject 時，合法和惡意基地台發送的信號強度在 SIB1 和 Attach Reject 之間存在明顯差異。因此，我們使用偵測器透過比較 SIB1 和 Attach Reject 之間信號強度的最大差異來識別 Attach Reject 攻擊，其偵測準確率為 91%。藉由我們利用惡意基地台發送的訊號強度較不穩定之特性所設計的機制，不僅可以解決以往研究的各種誤判情形，也可以提高識別在 4G LTE 中惡意基地台攻擊的準確率。此外，當我們將判斷資訊回應給 MEC 之後，MEC 也可以大範圍地通知有註冊此服務的用戶 APP，讓專網內的使用者可以得知惡意基地台攻擊的出現，減少可能的損失。

貳、文獻探討

隨著人們在生活中廣泛使用 4G 技術，許多攻擊者利用自己創建的惡意 4G 基地台進行惡意攻擊，對公眾造成危害。因此，在企業專網的資安議題，惡意基地台攻擊的偵測是需要迫切關注的。本章節將探討惡意基地台攻擊模型和現有的偵測方法。

2.1 企業專網

企業專網 (Non-Public Network, NPN) [10] [9] 的理念漸漸地推出，各大電信商也推出了四大種類的企業專網 [31][24] [5] [15] 共用型專網、專用型專網、獨立型專網以及切片型專網，其中電信商為了實施專用服務，會將基地台架設於企業專網環境中，使設備與 IoT 都與同一個基地台做連接，進而達到專屬的服務。電信商為了降低延遲會在基地台之後建設 MEC，把些許應用服務放置 MEC，迅速提供服務給用戶端。

2.2 多接取邊緣運算 MEC

MEC 建置於基地台 (Base Station, BS) 與核心網路 (Core Network) 之間，並且將核心網路部分服務，下放至 MEC 中以達到低延遲。如[17], [18] 等人建置，透過拆解封包了解使用者想請求的服務或者網站，並透過代理伺服器以及重定向流量的方法回覆使用者，進而達到降低服務請求的延遲性。因此電信商透過 MEC 的拆裝封包進而達到低延遲並且可以將流量進行資安分析來達到企業專網的安全。

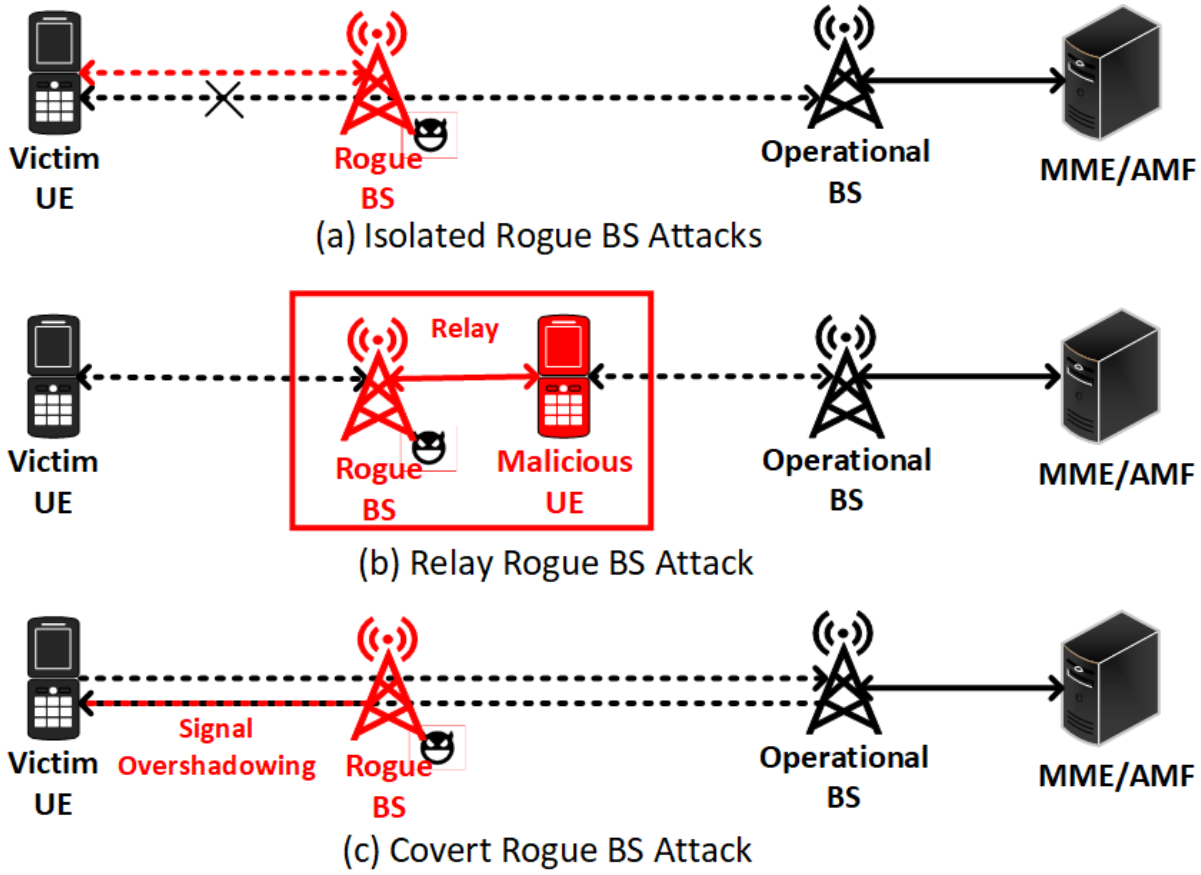

圖 1：惡意基地台攻擊

2.3 惡意基地台攻擊

我們將惡意攻擊行為統整為三個類型並詳加介紹，如圖 1。

2.3.1 獨立式惡意基地台攻擊

自從 2016 年獨立惡意基地台的惡意攻擊出現後[26]，近年來很多研究和實驗平台[7], [16], [29] 也採用這樣的方法實現各種信令攻擊。獨立的惡意基地台透過偽造附近的合法營運商欺騙受害者。此外，惡意基地台會使用更高的訊號強度引誘受害 UE，因為 UE 會不斷測量附近基地台的訊號強度及品質並擇優發送請求與進行連接。完成連線之後，攻擊者可以修改在 AKA 前未加密的信令，並基於該信令進行攻擊，讓受害 UE 接收和解碼。

2.3.2 中繼式惡意基地台攻擊

惡意基地台只能專注於未加密的信令，而 2018 年提出的中繼惡意基地台 [12] 實現了對加密信令和數據傳輸的攻擊。攻擊者使用惡意的基地台和 UE 來實施此類攻擊。這個中繼節點需要兩個 SDR 環境，一側是基地台，另一側是手機。例如，在上行數據傳輸過程中，惡意基地台會接收到受害者的請求，並透過解封裝 (decapsulation) 得到上層加密的封包。但是惡意基地台因為無法獲取到 KUPenc，所以無法對加密封包進行解封裝。但惡意基地台可以任意修改封包，因為數據傳輸沒有做完整性保護。然後將修改後的資料傳輸到中繼內的手機，最後將資訊封裝後發送到運營商運營的基地台[26]。

在這樣的情境下，電信營運商不知道攻擊者的存在，也無法確認上行資料傳輸是否有被更動。因此，這種方式可以實現中繼攻擊與中間人 (Man in the Middle, MITM) 攻擊。

2.3.3 遮蔽式惡意基地台攻擊

獨立的惡意基地台攻擊的缺點是無法持續攻擊。一旦攻擊者使用到需要與核心網路溝通的信令，攻擊就會曝露且中斷。這是因為獨立的惡意基地台無法讓使用者與核心網路連線，所以僅能利用部分的非加密信令做攻擊。且突然誘使受害 UE 連接並在攻擊後消失的模式也很容易被偵測。

因此，KAIST 團隊在 2019 年設計了遮蔽式惡意基地台攻擊 [32]，透過偽造信號覆蓋部分合法信號。惡意基地台需要在受害 UE 上同步來自當前合法基地台的信號頻率。當 UE 接收到兩個重疊的信號時，UE 將對來自惡意基地台較強的訊號做解碼。該方法透過在合法基地台上隱藏惡意基地台，可以持續覆蓋合法信號並修改下行數據。此外，受害 UE 還可以繼續透過上行傳輸與合法基地台通訊。因此，這種攻擊不容易被發現。同時，它會降低惡意基地台的功耗。但是，要實現這種類型的攻擊需要研究信號處理，比如了解合法基地台和受害 UE 的角度和位置，以達到精確的時間同步 (LTE 的 subframe 為 1ms)。

2.3.4 獨立的惡意基地台使用 Attach Reject 訊息達成 DoS 攻擊

使用獨立的惡意基地台針對 Attach Procedure 漏洞可以實現阻斷式服務 (Denial of Service, DoS) 攻擊 [12], [14], [21], [28]。

方法是當 UE 想要尋求服務時，會開始搜索附近基地台所廣播的同步信號 (Synchronization Signal)，以同步實體層的基本資訊後，UE 會以最高功率基地台建立的物理廣播通道 (Physical Broadcast Channel) 進行解碼，以得到主訊息區塊 (Master Information Block, MIB) 與系統資訊區塊 (System Information Blocks, SIBs) 的物理層帶

寬訊息。當 UE 與選定的基地台建立連接時，UE 會經由基地台向 MME 發送帶有 Attach Request 訊息的連接請求。並且此訊息將包含用戶隱私資料，例如 IMSI 和 IMEI。當 MME 驗證 UE 的身份後，會回傳 Authentication Request 進行後續的 AKA 驗證機制。當 MME 驗證 UE 的身份後，會回傳 Authentication Accept 來執行後續基於鑑權和密鑰管理的 AKA 驗證機制。此外，它是使用用戶和網路之間的相互認證，並透過密鑰

保護控制層 (Control Plane) 和用戶層 (User Plane) 的資料。然而，AKA 驗證機制後的信令難以獲得，因為它會被加密。因此，大多數攻擊是使用在 AKA 之前的明文信令來實施惡意攻擊。

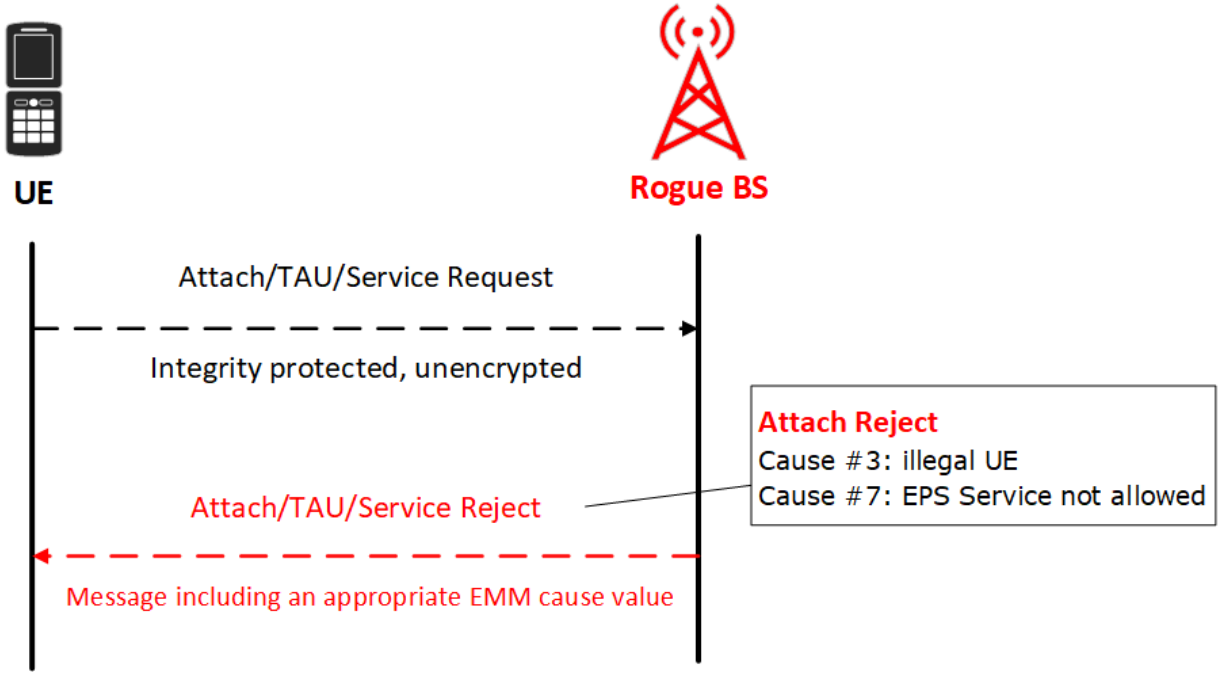

圖 2：Attach Reject 攻擊

根據 LTE 規範，在 AKA 之前仍然有很多不需要完整性保護的訊息。因此，攻擊者可以構建惡意基地台來偽造這些訊息，例如 Attach/TAU/Service Reject 訊息。當 UE 從 NAS 層向惡意基地台發送 Attach/TAU/Service Request 訊息時，攻擊者可以用 Attach/TAU/Service Reject 訊息進行響應以拒絕服務，因為 UE 可以在沒有完整性保護的情況下接受這些訊息。如圖 2 所示，惡意基地台將包含 EMMcause#7 的“EPS Service Not Allowed”加到 Attach Reject 訊息中，使得 UE 認為請求的服務無效。UE 收到拒絕之後，在重啟之前不會主動連接附近的其他合法基地台，從而實現 DoS 攻擊。

表 1：惡意基地台偵測文獻

Detector Category	Reference	Detected Parameters						
		PHY		RRC				NAS
		(1) RSRP	(2) SINR	(3) BS ID	(4) BS GPS	(5) BS GPS & ID	(6) Neighbor's BS ID	(7) Msg Sequence
Device Based	[1]	V		V		V	V	
	[3], [33]	V		V			V	
	[8]							V
Network Based	[13], [22], [30]	V					V	
Based Server Based	[6]		V					
	[23]	V		V		V	V	
	[25]	V		V		V		
	[20]	V		V				
	[11]	V			V			
	[27]	V						
	Our work	V						V

2.4 惡意基地台偵測

如表 1 所示，已經有許多研究有關於惡意基地台的偵測。我們將上述研究所用的網路層面分為以下三類。

2.4.1 PHY 層

雖然基地台發送的 PHY 層參數修改難度大，但獲取容易。而且，攻擊者通常會使用更高的信號強度來誘使受害 UE 連接到惡意基地台。因此，我們可以透過設備或蜂巢網路中的測量報告來接收 PHY 層的 RSRP。在現有的偵測機制中 [1], [3], [20], [22], [23], [25], [27], [30], [33]，幾乎所有 device-based、network-based 和 server-based 的偵測器都使用從 PHY 層接收到的 RSRP 來進行判斷，RSRP 是來自基地台的信號強度。他們透過比較是否高於多少 dBm 或超出哪個 dBm 的範圍來偵測惡意基地台的存在。

2.4.2 RRC 層

由於來自 RRC 層的訊息都是以明文進行傳送，因此最容易獲取和修改。我們可以從 device 得到的 RRC 訊息是當前正在連接或是裝置附近基地台的 BS ID。然而，network-based 的偵測器可以使用 UE 定期回傳給基地台的 measurement report 來獲得

相鄰基地台的 BS ID。這種偵測方法透過比對上述 RRC 訊息與合法基地台訊息來偵測出惡意基地台。但是我們需要透過其他資源獲取所有合法基地台訊息，例如從公共平台獲取合法基地台的 BS ID。並將這些數據與從 device 或 network 獲取的當前基地台的 BS ID 進行比對，以驗證當前連接的基地台的 BS ID 是否合法 [1], [3], [20], [23], [25], [33]。此外，我們還可以透過驗證相鄰基地台的 BS ID 來偵測惡意基地台 [1], [3], [22], [23], [30], [33] 及從公開資源獲取合法基地台的實體 GPS 位置 [1], [23], [25]，並使用設備的定位來確定位置是否匹配。

2.4.3 NAS 層

由於來自 NAS 層的流量更難獲取和解碼，在現有的偵測方法中，只有 Echeverria 等人開發了一個名為 Phoenix [8] 的 Android 應用程式，透過在設備上運行名為 MobileInsight [19] 的應用程式來接收來自 NAS 層的訊息。Phoenix 藉由分析接收到的 NAS 層訊息的順序是否符合 LTE 標準流程來識別惡意攻擊的可能性。例如，在 4G 通訊規範中，RLF Report 訊息僅在 AKA 身份驗證後出現。因此，如果 UE 在 Security Mode Command 訊息之前收到來自基地台的 RLF Report，則表示存在 RLF Report 攻擊。

參、系統架構

我們使用開源軟體 srsRAN 以及具穩定供電的軟體定義無線電設計一個可偵測惡意基地台攻擊的裝置偵測器。這個偵測器可以收集來自真假基地台的網路資料，並藉由收到的 Attach Reject 訊息與訊號強度來判斷是否來自惡意基地台。我們也有基於 Mobileinsight 開發 APP 來判斷是否有惡意基地台，如圖 3 所示，系統三個元件為：

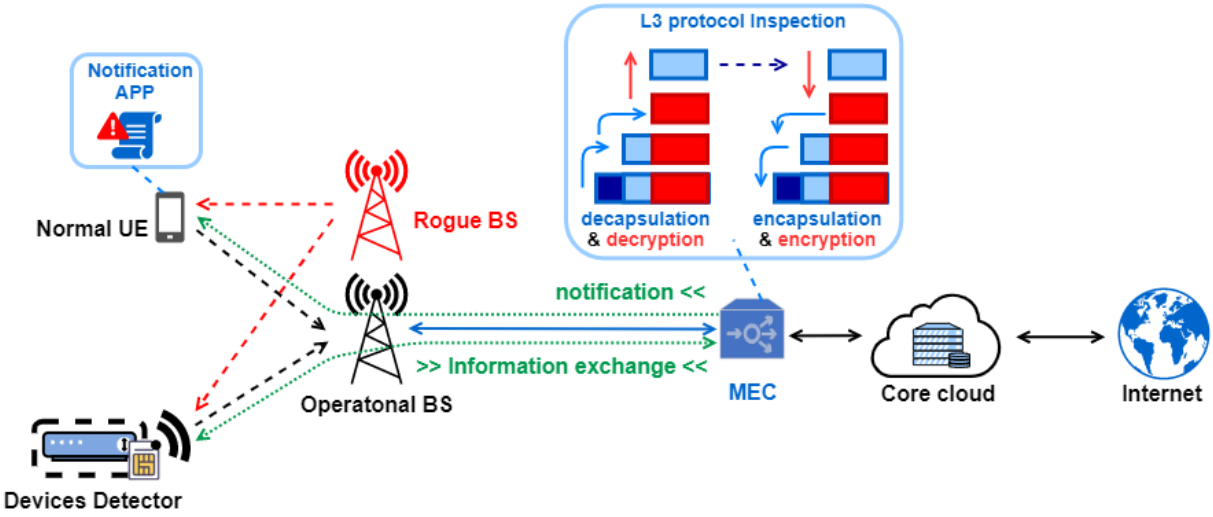

圖 3：系統架構

3.1 網路營運商提供的企業專網服務

為了分辨收到的 Attach Reject 訊息是否來自合法基地台，我們必須先在企業專網環境中收集真實基地台所發送的信令，並切在企業專網中的 MEC 設置我們的服務，當接受到來自偵測的警訊時，顯示在 MEC 的網頁上並且發通知給使用我們 APP 用戶。

3.2 具惡意攻擊的偽造基地台

本論文是採用獨立式的惡意基地台發送 Attach Reject 達到阻斷服務的攻擊。在本文的攻擊場景中，攻擊者無法利用實體層的訊號來覆蓋掉合法的信號，因此只能藉由發送比合法基地台更強的訊號功率吸引受害者 UE 連接到惡意基地台，且惡意基地台可以廣播與合法基地台相同的 MIB 和 SIB1/2 訊息，也可以更改 Cell ID、MCC、MNC 等訊息使其與合法基地台相同，以冒充合法的網路營運商，向 UE 注入惡意訊息。

3.3 基於裝置的可識別惡意攻擊的偵測器

我們設計的偵測器是基於裝置來進行數據的收集與分析。首先利用裝置收集來自真實合法基地台與偽造基地台的資料，並將其視為訓練資料集。再來計算每筆訓練集中的 SIB1 到 Attach Reject 間的最大訊號強度差，並將這些差值的平均用來作為最後判斷真假基地台的 threshold (標註為 th)。最後，當裝置執行收集 real-time 的信令並進行解碼時，如果發現收到 SIB1 到 Attach Reject 的訊號功率最大差異值大於訓練資料集計算出的 th 時，即判斷此訊息存在異常行為，並在裝置的執行畫面中出現警示，告知使用

者目前連線的蜂巢網路具有惡意的 Attach Reject 攻擊行為，並將偵測結果回傳至 MEC。

在企業專網中也放置我們基於 Mobileinsight 開發的 APP，不斷偵測企業專網環境中是否有惡意基地台，若有收到來自惡意的訊息，在本地端發起警訊告知身邊的人外，也當連回至合法基地台之後，會將訊息傳至 MEC。

肆、實驗方法

在本節中，我們將描述實驗平台中使用的軟體和硬體設備，以及我們設計的偵測方法。

圖 4：實驗平台

4.1 軟體與硬體設備

4.1.1 硬體設備

如圖 4 所示，我們使用兩台配有相同 Intel Core i5 6500 CPU、4 核和 24GB RAM 的主機，加上兩個軟體定義無線電與四根天線來模擬一個在企業專網中有著 UE 以及 MEC 還有偵測器。此實驗環境使用的 SDR 型號為 USRP-B210。如圖 5 所示，我們使用一台與上述相同的主機，並且使用 B210 來進行攻擊。

4.1.2 軟體元件

我們利用上述設備運行以下兩個主元件傳送偽造信令的惡意基地台我們在主機中使用開源軟體 srsRAN，並結合 SDR 和天線構建一個惡意基地台。另外，透過修改惡意基地台中的 NAS 層配置，當受害設備向惡意基地台發送 Attach Request 時，惡意基

地台可以回傳 Attach Reject 來拒絕該設備的服務。之後，受害者將被釋放，並且不會對蜂巢網路重新請求連線直到它重新啟動，以達到拒絕服務的目的。設備端的偵測器: 我們在主機上運行 srsUE 並使用商用 SIM 卡結合 SDR 來與基地台連線，進行監測環境中是否有惡意基地台，並且將結果傳送到 MEC。

圖 5：攻擊平台

4.2 實驗過程

因是實驗環境，所以我們使用 srsRAN 構建了一個企業專網的環境以及 MEC，並且設計一種基於設備的偵測器，也使用 srsRAN 開發一個具發送惡意 Attach Reject 訊息的惡意基地台。偵測器使用商用 SIM 卡從合法基地台中收集資訊後，接回我們架設的企業專網中，進而判斷是否收到來自惡意基地台的攻擊，如圖 6，我們將偵測器分析過程分為以下三個步驟：

4.2.1 資料蒐集

我們使用 srsUE 結合 SDR 接收來自合法和惡意基地台的訊息。由於提供 SDR 使用的電源會影響訊號功率，因此我們使用額外的穩定電源以確保訊號的品質。

為了收集真實 Attach Reject 訊息，我們使用 srsUE 結合過期的商用 SIM 卡向合法運營商請求服務。此外，我們使用 srsRAN 構建了一個惡意基地台來獲取惡意的 Attach Reject 訊息。在這個數據收集步驟中，我們從合法和惡意基地台收集了 20 筆 Attach Reject 訊息。

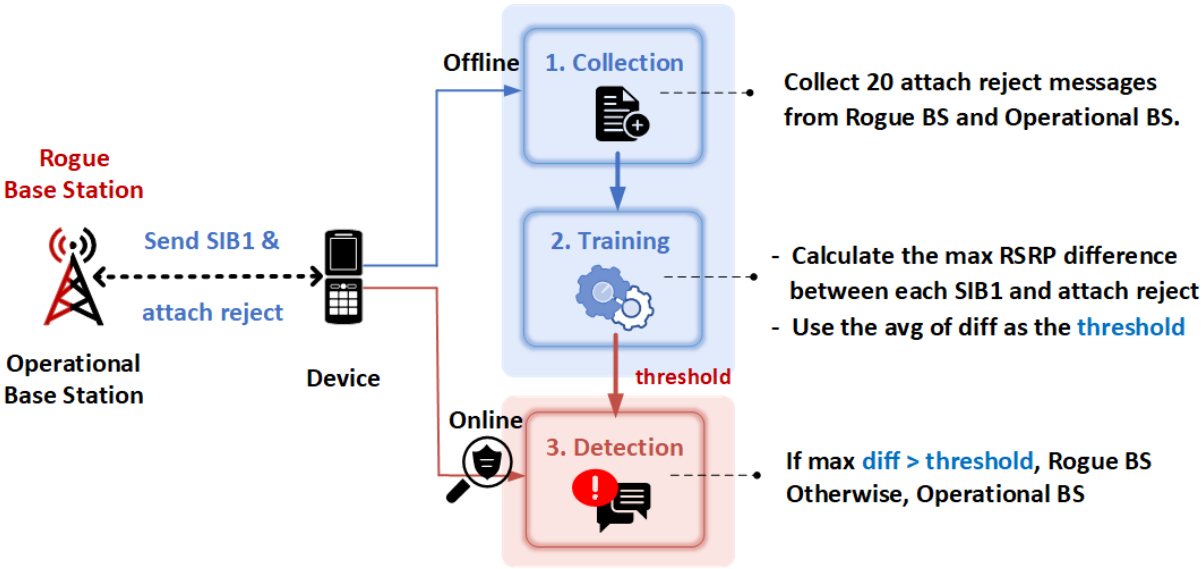

圖 6：實驗流程

4.2.2 資料訓練

由於大多數惡意基地台發送的信號強度相對不穩定，並且基地台會定期廣播 SIB1 訊息，因此我們從數據收集階段計算每個 SIB1 和 Attach Reject 之間的最大信號強度差。此外，我們將計算出的差異取平均值作為識別合法和惡意基地台的 threshold th。我們標記了從惡意基地台和合法基地台接收到的 SIB1 時的信號強度為 ⟦rsrp⟧_(r,SIB1) 和 ⟦rsrp⟧_(l,SIB1)。另外，Attach Reject 時的信號強度為 ⟦rsrp⟧_(r,AR)和 ⟦rsrp⟧_(l,AR)。之後，我們計算了從惡意基地台和合法基地台接收到的 SIB1 和 Attach Reject 的信號強度差異，分別如公式 (1) 所示：

$$\begin{cases} diff_r = rsrp_{r,\mathrm{SIB1}} - rsrp_{r,\mathrm{AR}}, & \text{Rogue BS} \\ diff_l = rsrp_{l,\mathrm{SIB1}} - rsrp_{l,\mathrm{AR}}, & \text{Legitimate BS} \end{cases} \quad (1)$$

為了避免結論的偏移，我們對惡意基地台與合法基地台個別搜集了 n 筆資料，並且算出 threshold，如第 (2) 式所示：

$$th = \sum_{i=0}^{n} \frac{diff_r + diff_l}{n} \quad (2)$$

4.2.3 資料偵測

在數據偵測階段，我們從實驗基地台收集 SIB1 和 Attach Reject 訊息的 RSRP (分別標記為$rsrp_{\mathrm{SIB1}}$ 和$rsrp_{\mathrm{AR}}$)，並計算其差值 $diff$，如 (3) 式：

$$diff = rsrp_{\mathrm{SIB1}} - rsrp_{\mathrm{AR}} \quad (3)$$

最後，如公式 (4) 所示，當差異值 $diff$ 超過訓練階段計算出的 th 時，接收到的 Attach Reject 將被視為來自具有惡意攻擊行為的惡意基地台。相反，則它來自一個合法的基地台。

$$\text{Result} = \begin{cases} \text{Rogue BS}, & \text{if } diff \geq th \\ \text{Legitimate BS}, & \text{otherwise} \end{cases} \quad (4)$$

伍、實驗結果

我們目的是設計一種在企業專網環境中使用基於設備的偵測器，可以偵測惡意基地台的攻擊，並利用惡意基地台的不穩定的信號強度來偵測 NAS 層漏洞的惡意 Attach Reject 攻擊並評估準確性，最後將結果回傳至 MEC，再傳送給使用者警訊。

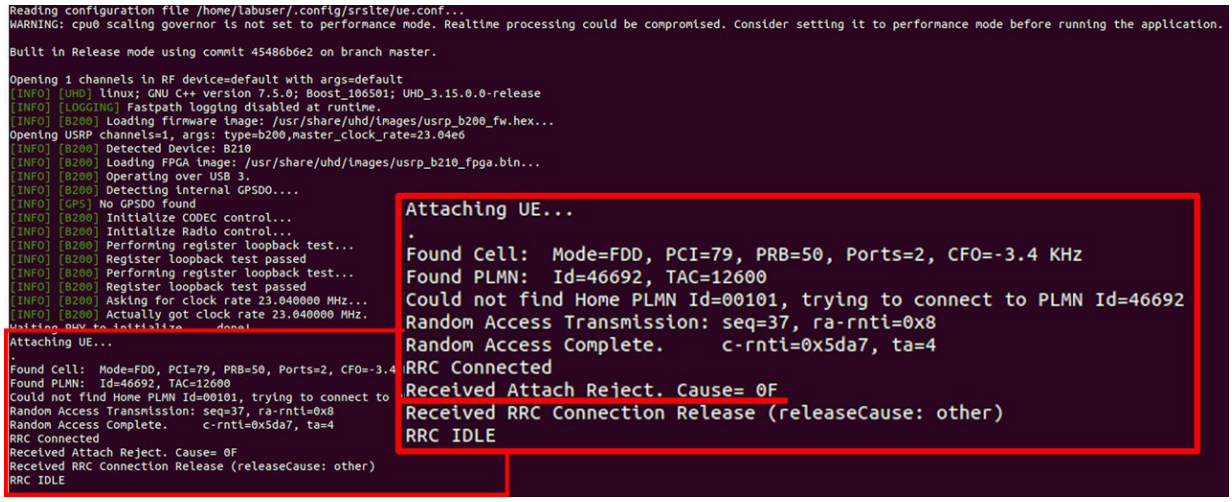

圖 7：偵測器接收基地台發的 Attach Reject 訊息

5.1 偵測器從 BS 接收 Attach Reject

圖 7 顯示使用 srsUE 設計的移動設備從合法和惡意基地台接收 Attach Reject 訊息。

5.2 合法與惡意基地台信號功率分析

收集基地台發送的 Attach Reject 後，我們分析這些數據中的信號功率。圖 8 顯示了信號強度在時間軸上的分佈。

我們可以注意到，惡意基地台使用的功率並不總是高於合法基地台的功率。而從這次攻擊中，設備從基地台收到 Attach Reject 後，信號功率會迅速下降。我們認為可能是因為合法基地台發送 Attach Reject 後拒絕服務並斷開設備，導致設備接收到的信號功

率下降。另外我們可以觀察到，惡意基地台發送的功率差比合法基地台要大很多，但穩定性相較比較差。

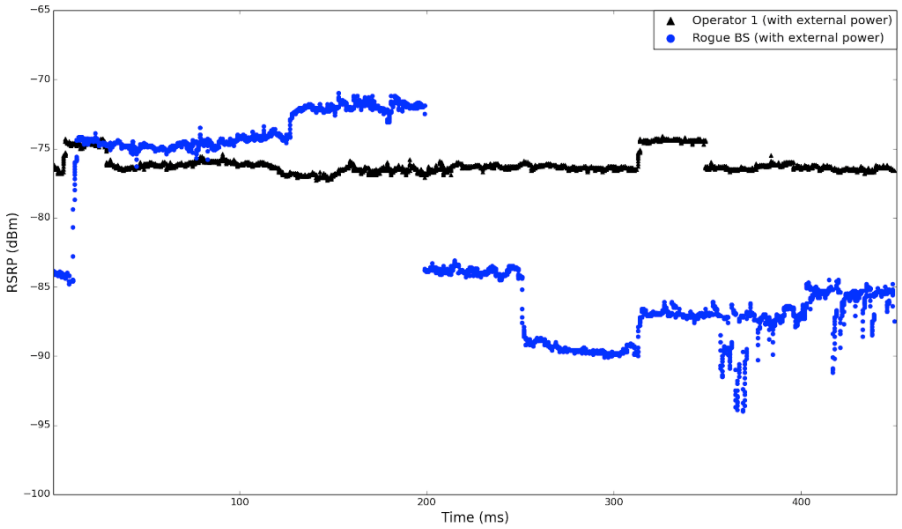

圖 8：真偽基地台之訊號功率分析示意圖

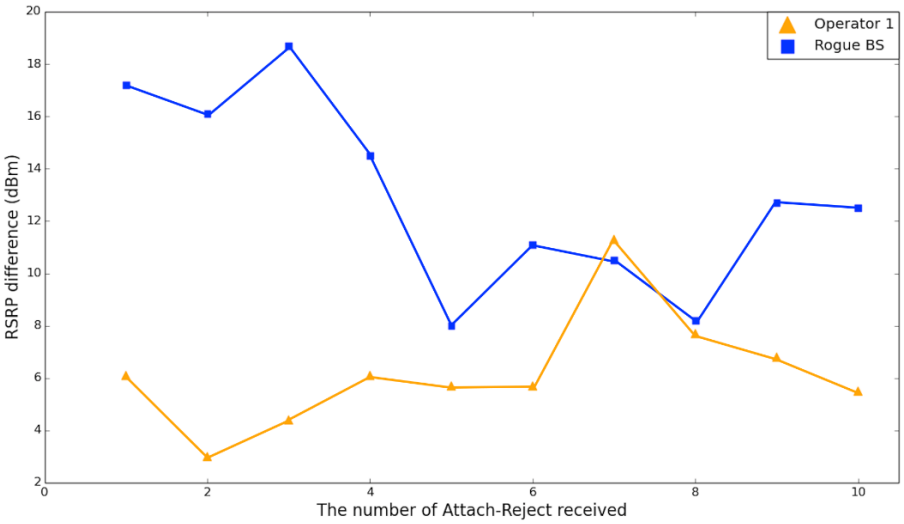

圖 9：SIB1 到 Attach Reject 間的訊號功率差異圖

5.3 合法與惡意基地台信號功率差異分析

如圖 9，通過計算 SIB1 和 Attach Reject 的最大信號強度差異，可以觀察到惡意基地台的差異值比起合法基地台來得更高。我們認為原因是惡意攻擊者通常使用好攜式 SDR 發送信號以方便移動。但是，這些低成本的 SDR 硬體規格比合法基地台差，導致惡意基地台發送的信號強度不穩定。

為了測量 SIB1 和 Attach Reject 之間信號強度差異，我們使用統計中常用的標準差 σ，如等式 (5) 所示：

$$\sigma = \sqrt{\frac{1}{n}\sum_{k=1}^{n}(x_i - \bar{x})^2} \qquad (5)$$

如表 2 所示，惡意基地台的 SIB1 和 Attach Reject 之間差異的標準差明顯高於合法基地台。因此，我們認為可以通過該區間的信號功率差異來判別惡意基地台。

表 2：真偽基地台之訊號強度差異標準差

SIB1 to Attach Reject	Operator	Rogue BS
Standard Deviation	7.44	36.52

5.4 設備端的偵測器

圖 10 顯示偵測器會計算 SIB1 和 Attach Reject 之間的信號最大功率差異值，判別來自合法或惡意基地台的訊息。

在評估階段，我們採用一般評估指標來評估我們提出的方法與性能。這些指標是根據以下定義的。

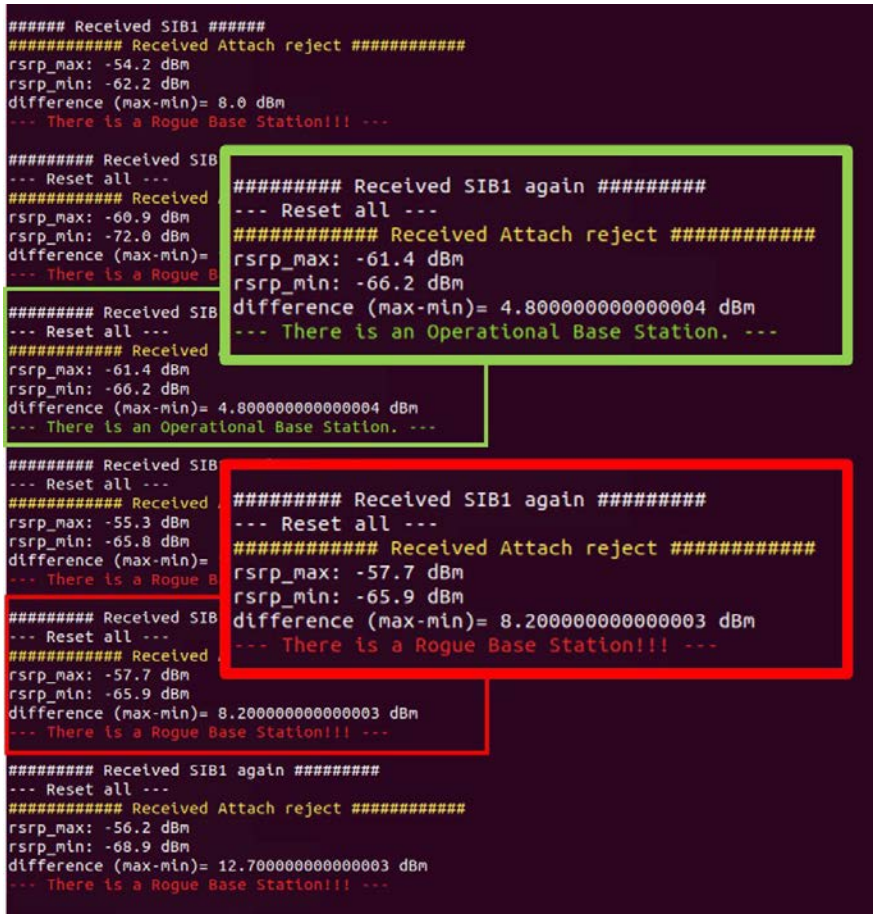

圖 10：偵測器判斷合法/惡意基地台之示意圖

- True positive (TP) : samples correctly classified as positive.
- False positive (FP) : samples incorrectly classified as positive.
- True negative (TN) : samples correctly classified as negative.
- False negative (FN) : samples incorrectly classified as positive.

Accuracy refers to the proportion of correct judgments of true and false:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{n}} \qquad (6)$$

Precision refers to how much is true when the judgment is true:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \qquad (7)$$

Recall is the probability of the samples in the positive class being classified correctly:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \qquad (8)$$

F1-measure is the weighted average of precision and recall:

$$\text{F}_1\text{\_measure} = \frac{2 * (\text{Recall} * \text{Precision})}{\text{Recall} + \text{Precision}} \qquad (9)$$

表 4 偵測器偵測出惡意基地台攻擊之準確率

Accuracy	Precision	Recall	FPR
91%	91.83%	90%	8%

從表 4 可知我們的偵測器判別惡意基地台發送的 Attach Reject 攻擊之準確率 (Accuracy) 為 91%。透過我們的實驗可驗證相較於其他篇只根據某一層參數的偵測器，我們針對惡意基地台發送 PHY 層中的訊號強度不穩定的特性，並且結合 NAS 層的訊息，所實現的的 4G LTE 網路中偵測機制，會來的更加準確。

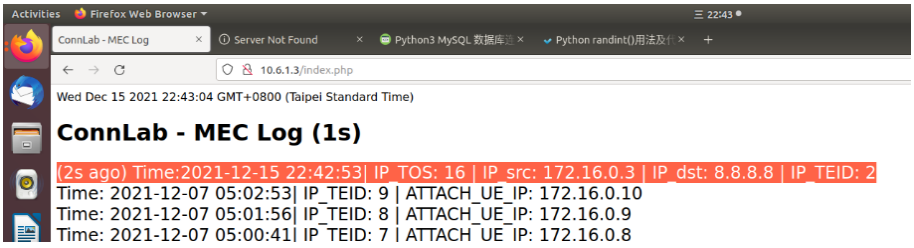

圖 11：偵測成功後回傳到 MEC 上

5.5 MEC 上的網頁

從圖 11 中可以看見，當我們的偵測端偵測到惡意訊息之後，除了在本地端顯示警訊之外，偵測器回到合法基地台之後，會將偵測結果上傳到 MEC 上，並且在 MEC 的網站上顯示已收到偵測器的警告。

5.6 回傳至使用端

當 MEC 收到偵測端發送的警訊後，會發出通知到我們使用者的手機上，並且使用者需使用我們開發 APP，將會收到如圖 12 所示畫面。

圖 12：使用者上的警訊

陸、結論與未來工作

在本文中，我們旨在企業專網的環境中透過偵測器使用惡意基地台的信號強度不穩定的特性，通過 PHY 層的最大參考信號接收功率 (RSRP) 的差異值來區分來自合法基地台或惡意基地台的 NAS 層消息。在我們的實驗中，我們使用 NAS 層漏洞來實施拒絕攻擊作為偵測目標。我們使用開源軟件 srsRAN 和低成本的 SDR 來建置一個可以發送惡意 Attach Reject 消息的惡意基地台。

此外，我們使用 srsUE 和商業 SIM 卡來設計基於設備的偵測器，並使用 SDR 接收來自合法和惡意基地台的信令。此外，我們提出了一種偵測機制以及警告方法，通過計算 SIB1 和 Attach Reject 之間的最大 RSRP 差異值來識別惡意基地台攻擊，以區分來自 NAS 層的 AttachReject 消息，除了本地端警告之外，還會再透過 MEC 發送通知給予使用我們服務的使用者。實驗結果表明，我們的偵測機制可以 91% 的準確率偵測惡意基地台攻擊。因此，我們認為我們的機制不僅可以偵測 Attach Reject 攻擊，未來還可以偵測具有 RSRP 不穩定特徵的其他惡意攻擊。

[誌謝]

本論文的部分成果是由科技部「【國際合作鏈結法人計畫】：5G 多接取邊緣計算之存取控制」 (計畫編號：109-2923-E-011-006-MY3) 與「利用軟體無線電研究 5G 虛擬線電接取網路之安全」 (計畫編號：108-2628-E-011-007 -MY3) 和經濟部「以 SDN/NFV 來帶動 IoT 與 5G 之創新和服務計畫」 (計畫編號：109-EC-17-A-02-S5-007) 的支持。

參考文獻

[1] Android IMSI-catcher detector. https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/. Accessed: 2021-04-04.

[2] Fake antenna detection project. https://fadeproject.org/. Accessed: 2021-04.

[3] Snoopsnitch. https://opensource.srlabs.de/projects/snoopsnitch, 2019.Accessed: 2021-04-04.

[4] 3GPP. System Architecture Evolution (SAE) , Security architecture.Technical Specification (TS) 33.401, 3rd Generation Partnership Project (3GPP) , 01 2010. Version 9.2.0.

[5] A. Aijaz. Private 5G: The future of industrial wireless. IEEE Industrial Electronics Magazine, 14, Dec. 2020.

[6] A. Ali and G. Fischer. Enabling fake base station detection through sample-based higher order noise statistics. In Proc. TSP 2019, pages 695–700, July 2019.

[7] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik. New privacy threat on 3g, 4g, and upcoming 5g aka protocols. Proc. Privacy Enhancing Technologies, 2019 (3) :108–127, Nov. 2019.

[8] M. Echeverria, Z. Ahmed, B. Wang, M.-F. Arif, S.-R. Hussain, and O. Chowdhury. PHOENIX: Device-centric cellular network protocol monitoring using runtime verification. In Proc. NDSS 2021, Jan. 2021.

[9] M. H. C. Garcia, A. Molina-Galan, M. Boban, J. Gozalvez, B. CollPerales, T. Şahin, and A. Kousaridas. A tutorial on 5G NR V2X communications. arXiv preprint arXiv:2102.04538, Feb. 2021.

[10] S. Garg, K. Kaur, G. Kaddoum, and K.-K. R. Choo. Toward secure and provable authentication for internet of things: Realizing industry 4.0. IEEE Internet of Things Journal, 7, May 2019.

[11] K.-W. Huang and H.-M. Wang. Identifying the fake base station: A location based approach. IEEE Commun. Lett., 22 (8) :1604–1607, Aug. 2018.

[12] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In Proc. NDSS Symposium 2018, Feb. 2018.

[13] L. Karaçay et al. A network-based positioning method to locate falsebase stations. IEEE Access, 8:111368–111382, Aug. 2021.

[14] H. Kim, J. Lee, E. Lee, and Y. Kim. Touching the untouchables: Dynamic security analysis of the LTE control plane. In Proc. IEEESP 2019, pages 1153–1168, May 2019.

[15] C. Lai, R. Lu, D. Zheng, and X. S. Shen. Security and privacy challenges in 5G-enabled vehicular networks. IEEE Network, 34, Apr. 2020.

[16] G. Lee et al. This is your president speaking: Spoofing alerts in 4G LTE networks. In Proc. ACM MobiSys 2019, pages 404–416, June 2019.

[17] C.-Y. Li, Y.-D. Lin, Y.-C. Lai, H.-T. Chien, Y.-S. Huang, P.-H. Huang, and H.-Y. Liu. Transparent AAA security design for low-latency MEC-integrated cellular networks. IEEE Transactions on Vehicular Technology, 69 (3) :3231–3243, January 2020.

[18] C.-Y. Li, H.-Y. Liu, P.-H. Huang, H.-T. Chien, G.-H. Tu, P.-Y. Hong, and Y.-D. Lin. Mobile edge computing platform deployment in 4G LTE networks: A middlebox approach. In Proc. USENIX Workshop 2018, June 2018.

[19] Y. Li, C. Peng, Z. Yuan, J. Li, H. Deng, and T. Wang. Mobileinsight:Extracting and analyzing cellular network information on smartphones. In Proc. ACM MobiCom 2016, pages 202–215, Oct. 2016.

[20] Z. Li et al. FBS-Radar: Uncovering fake base stations at scale in the wild. In Proc. NDSS, Jan. 2017.

[21] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar. Survey on threats and attacks on mobile networks. IEEE Access, 4:4543–4572, Aug. 2016.

[22] P.-K. Nakarmi, M.-A. Ersoy, E.-U. Soykan, and K. Norrman. Murat: Multi-RAT false base station detector. arXiv preprint arXiv:2102.08780, Feb. 2021.

[23] P. Ney, I. Smith, G. Cadamuro, and T. Kohno. SeaGlass: enabling citywide IMSI-catcher detection. Proc. Sciendo PETS 2017, 2017 (3) :39–56, March 2017.

[24] J. Ordonez-Lucena, J. F. Chavarria, L. M. Contreras, and A. Pastor. The use of 5G Non-Public Networks to support industry 4.0 scenarios. In Proc. CSCN 2019, Dec. 2019.

[25] Quintin and Cooper. Detecting fake 4G LTE base stations in real time. In Proc. USENIX Association 2021, Feb. 2021.

[26] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper. Breaking LTE on layer two. In Proc. IEEE SP 2019, pages 1121–1136, May 2019.

[27] M. Saedi et al. Generation of realistic signal strength measurements for a 5G rogue base station attack scenario. In Proc. IEEE CNS 2020, pages 1–7, June 2020.

[28] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert. Practical attacks against

privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:1510.07563, Aug. 2017.

[29] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert. On the impact of rogue base stations in 4G/LTE self organizing networks. In Proc. ACM WiSec 2018, pages 75–86, June 2018.

[30] S. Steig, A. Aarnes, V.-D. Thanh, and H.-T. Nguyen. A network based IMSI catcher detection. In Proc. IEEE ICITCS 2016, pages 1–6, Sept. 2016.

[31] E. C. Strinati, T. Haustein, M. Maman, W. Keusgen, S. Wittig, M. Schmieder, S. Barbarossa, M. Merluzzi, H. Klessig, F. Giust, et al. Beyond 5G private networks: the 5G conni perspective. In Proc. IEEE GLOBECOM, Mar. 2020.

[32] H. Yang, S. Bae, M. Son, H. Kim, S.-M. Kim, and Y. Kim. Hiding in plain signal: Physical signal overshadowing attack on LTE. In Proc. USENIX Security Symposium 2019, pages 55–72, Aug. 2019.

[33] P. Ziayi, S.-M. Farmanbar, and M. Rezvani. YAICD: Yet another IMSI catcher detector in GSM. Security and Communication Networks, 2021, Jan. 2021