低成本的 LTE 搜尋與探聽工具–使用簡易 SDR 硬體模擬假基地台

作者：李孟寰、王繼賢

國立中正大學

通訊工程學系

網路前瞻技術實驗室

mhlee@alum.ccu.edu.tw

指導教授：潘仁義 副教授

109 年 9 月 22 日

摘要

在過去，無線通訊的探聽與測量設備都相對昂貴且不易接觸，但隨著軟體定義無線電(Software Defined Radio, SDR)的發展，越來越多人能夠用較低的成本接觸到這些無線電設備，我們可以用現成的器材與個人電腦來執行非常多的功能與實驗，但這也可能讓無線網路更容易受到有心人士的攻擊。

透過簡易的 Linux 程式、現成的電腦和 SDR 設備，我們能夠以較低的成本，對周遭 LTE(Long Term Evolution ，長期演進技術)網路進行其重要參數的測量與封包探聽，並模擬假基地台，捕捉傳呼紀錄並獲取連線裝置的 s-TMSI、IMSI 等身分資訊，甚至利用 LTE 連線過程的漏洞作為可能的攻擊工具，影響正常連線，達到阻斷服務攻擊的效果。

這些除了會造成使用者不便外，更牽涉到隱私權的問題，甚至使電信商及客戶蒙受財務上的損失。

關鍵詞：軟體定義無線電(SDR)，長期演進技術(LTE)，假基地台，阻斷服務攻擊(DoS)，隱私權

目錄

1. 前言

1.1 研究動機

過往的無線通訊與 LTE 探聽器材價格較高，一般人不容易接觸與使用，比如由美國 Harris Corporation 所生產的 Stingray phone tracker 設備或是 SRS(Software Radio System) 開發的商用 LTE 分析軟體 AirScope 等，這些設備都動輒數千甚至上萬美元，硬體體積也較為龐大，隨著近幾年來無線通訊的演進與 SDR 的發展，只需要一般市售的 PC 與 RF 前端硬體，搭配開源軟體，就可實作非常多的功能，比如 srsLTE 就提供了 LTE 平台全協議層的實作，提供了更大的可能性。

這些都讓研究與實作成本大幅降低，但是，也可能被利用，對無線通訊的安全性產生一些問題。

我們使用 srsLTE 軟體平台[1]，與 Ettus 公司的 USRP(Universal Software Radio Peripheral) 軟體定義無線電(SDR)開發板[2]，來探討無線通訊可能的隱私與安全性問題。

我們嘗試透過 Linux 程式、現成的電腦和 SDR 開發板，證明用低的成本、基礎的 Linux 與電腦網路知識，能夠對周遭 LTE 網路進行探聽和測量，甚至進而模擬假基地台擷取 s-TMSI 與 IMSI 這兩項 UE 身分資訊。

1.2 相關作品

無線通訊的探聽與攻擊的相關研究從 2G/3G GSM 時代就已經存在，其中一類稱作 IMSI Catcher 或假基地台。剛進入到 4G LTE 時代時，LTE 因為有更好的認證演算法與認證機制，被視為是很安全的協議，不受此類攻擊威脅。但近年來越來越多學術研究指出[3-8]，創造針對 LTE 做攻擊的假基地台是可行的，且對其連線與安全性的干擾程度不亞於 GSM 時代假基地台攻擊造成的影響。

這類攻擊手法，主要包含干擾(jamming)或捕捉連線，利用協議漏洞揭露被害裝置位置或身分資訊，側聽封包流量等。以下相關學術研究都使用現有的開源軟體進行改造，比如 OpenLTE、srsLTE 與 Open Air Interface (OAI)等。

- Stig F. Mjølsnes 和 Ruxandra F. Olimid 在其研究中[3]改造 OAI，來利用 LTE 基地台選擇過程的漏洞，並建立假基地台來示範阻斷服務(Denial of Service,DoS)攻擊。
- Wooniety 在 Github 上公開了其利用 srsLTE library，抓取 Paging Records 來取得 UE 資訊，建立 LTE 竊聽裝置(sniffer)的原始碼。[8]

我們參考這些程式碼，來改造新版本的 srsLTE，執行相關的實驗。

2. LTE 行動網路

在本節中，我們會對於 LTE 行動網路的架構，以及其基本的連線機制，做概略的介紹，以幫助讀者了解本研究相關的背景知識。

2.1 LTE 網路架構

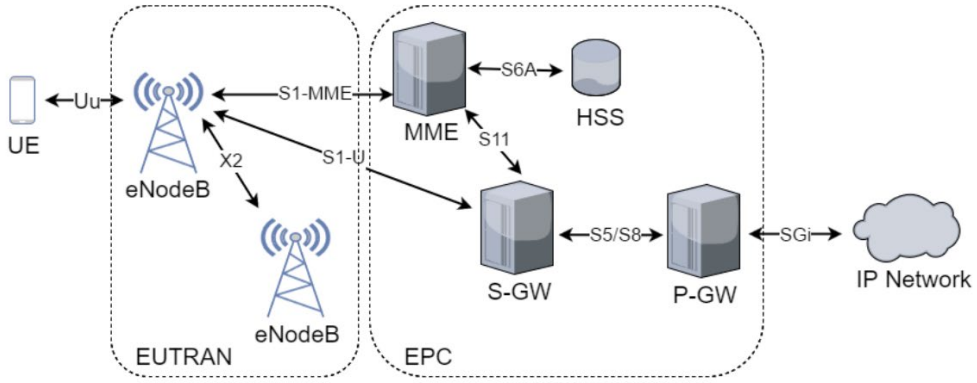


圖 1 LTE 網路架構[3]

LTE 的網路架構概略分成兩個部分:無線部分 EUTRAN (Evolved Universal Terrestrial Radio Access Network)與核心網路部分 EPC (Evolved Packet Core)。UE(User Equipment)指的是一個使用者的終端裝置，比如常見的智慧型手機。UE 內會裝有 USIM(Universal Subscriber Identity Module，通用用戶識別模組)，其中存有 IMSI（International Mobile Subscriber Identity，國際移動用戶識別碼）及與其關聯的用於認證與加密的密鑰。

- eNodeB (evolved NodeB) 是一個與 UE 透過無線電通訊的基地台，其作為網路服務中的無線接入點。
- MME (Mobile Management Entity) 負責認證與分配資源給 UE。
- HSS (Home Subscriber Server) 儲存認證用的資訊以及私鑰等 UE 的細節資訊。
- S-GW (Serving Gateway) 連接 EUTRAN 與 EPC 之間，
- P-GW (PDN Gateway)是與提供與外部 PDN(Public Data Network)連線的路由點。

行動網路的識別是透過 MCC（Mobile Country Code，行動裝置國家代碼）與 MNC（Mobile Network Code，行動網路識別碼）結合使用（也稱為「MCC / MNC」），其用來表示唯一一個的行動裝置的網路服務提供商。MCC 跟 MNC 的代碼都是公開的[10]。一個 eNodeB 控制一組使用一特定頻段--或等同於同一 EARFCN (EUTRA Absolute Radio-Frequency Channel Number)的基地台。每個電信商分配到的頻段也都是公開的資訊[11]。而在同一個地理區域的數個基地台

會形成一個 TAC(Tracking Area Code) ，由單一個 MME 管理。eNodeB 會透過定期廣播 SIB(System Information Block)訊息來傳遞 MCC、MNC 或 TAC 資訊。UE 會利用這些資訊來判別電信商。當要進行 attach 到網路時，UE 會傳送 ATTACH_REQUEST 給 eNodeB。若 UE 移動到了新的區域，它會啟動 TAU REQUEST 並執行 TRACKING AREA UPDATE 程序。
我們於此跳過其他細節[12]，將本專題的重點，著重於 UE 建立連線，以及進行 Paging 時的過程。

2.2 LTE 基地台選取與重選

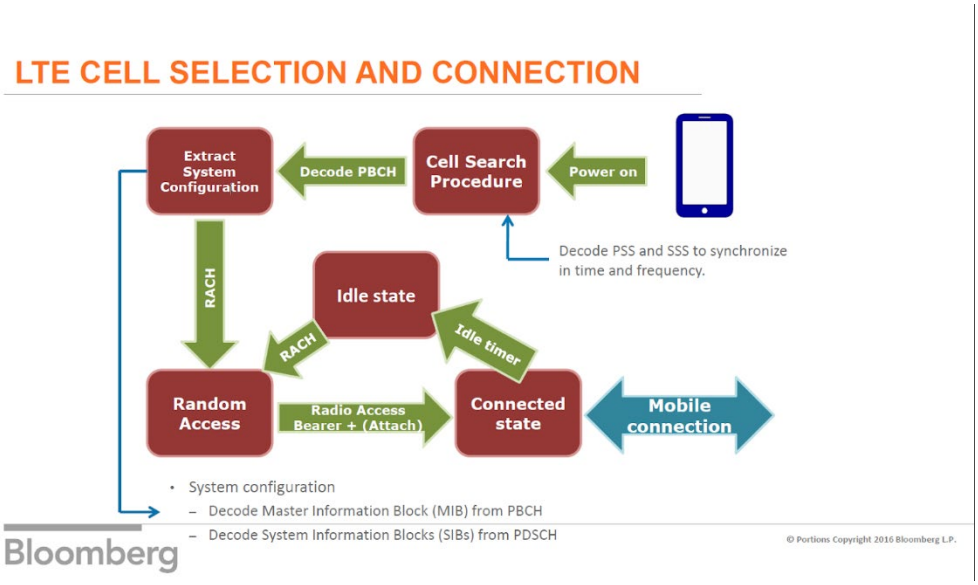


圖 2 LTE 的基地台選擇與連線過程[7]

當 UE 試圖連線到行動網路時，會先執行 *cell selection* 程序，其會找尋能提供最佳服務的基地台並與其建立連線。
若 UE 之後找到更適合的基地台(根據一些規則來判斷)，那其會執行重選 *(re selection)* 過程，兩基地台換手並建立新連線。選擇與重選基地台的過程包括許多的步驟並依靠不同的規則，我們在此並不會列出完整的細節，只會說明與我們的專題有關的部分。

當 UE 開啟時，會選擇在一 PLMN (Public Land Mobile Network，公用陸上行動網路)內的基地台，PLMN 由 MCC+MNC 組成，這個步驟透過存在本機上的 PLMN 列表與一些規則來決定。實務上 UE 會依據上次成功連線的結果來選擇適合的基地台，並不一定要是它的 HOME PLMN(USIM 本身所屬的電信商)。
在重選時，UE 會監測同頻段、不同頻段以及 RAT（Radio Access Technology，無線電接入技術)之間的基地台，這些資訊由目前的基地台提供。eNodeB 會定期透過 SIB 廣播基地台選擇的優先權順序(以及相關規則和參數)。UE 會遵照這些指示，盡可能的選取優先權最高的基地台或頻段。

電信商會透過優先權的排序來最佳化服務的可靠度，同一個區域內也會有多個不同頻段的基地台，避免故障或網路壅塞影響使用者。當高優先權的基地

台無法連線時，UE 可以依照下一個順位的條件來選取基地台，不會完全喪失連線。

2.3 LTE Paging 程序

UE 如果需要空中資源，必須要使用 RRC(Radio Resource Control)去要空中資源，使用的是 Random Access process，但是如果是網路端要透過 eNodeB 去找尋 UE(有時 eNodeB 也會直接做 Paging，例如 Tracking Area Update、System Information Update 等等)，就會使用 Paging[13]。

當網路端或 eNodeB 需要對 UE 進行資料傳送時，eNodeB 會對 UE 進行 Paging，這時 eNodeB 會在 PDCCH 中以 P-RNTI(Paging Radio Network Temporary Identifier，RNTI=0xfffe)夾帶 Paging 提醒的訊息，UE 符合 R-RNTI 者，會解碼 PDCCH 中資訊，內含 UE 要去 PDSCH 的哪個位置找 paging 的詳細資訊。

其中的 Paging Record 裡會紀錄 ue-Identity 這個欄位，以指定被呼叫的 UE 身分，其中 IMSI 或 s-TMSI 都可以用來標記 UE。

當 UE 找到 Paging 的詳細資訊後，會對 eNodeB 進行 Random Access Procedure，並進行 RRC Connection。

需要注意的是，由於 Paging Message 是由 P-RNTI 標記，同個 cell 內的所有 UE 都可以解碼，不同的 UE 如果發現 Message 中包含了 System Information Change 或是 ETWS(Earthquake and Tsunami Warning System，地震海嘯警告系統）和 CMAS（Commercial Mobile Alert Service，商用移動裝置預警系统）的訊息指示，都要進行相應的處理，這時 UE 是不需要將自己的 IMSI 或 s-TMSI 跟 Message 中的標記進行比對的。

2.4 安全性考量與實驗方法的設計

因為我們的目標是即便在低成本的限制下，希望取得越多隱私權資訊越好，雖然 Paging Message 內可以透過 IMSI 來識別 UE 身分，實務上因為安全性考量，都盡量以臨時的 s-TMSI 來傳遞，避免 IMSI 洩漏。所以除了單純解碼 Paging Message 外，我們也試著模擬假基地台，來進一步取得 IMSI 資訊。

3. 實驗設備與工具

為了實現簡易且低成本的目標，我們只使用現成的(Off-the-shelf)設備與軟體來進行實驗。

電腦設備 ：

- 一台 DELL Optiflex9020 i5-4570 CPU@3.2GHz
- 一台 Acer Aspire V3-371 i5-5200u CPU@2.2GHz
- OS 皆執行 Ubuntu 18.04, kernel 版本為 linux-5.4.0-39-lowlatency 。

並且有原生 USB3 連接埠(為避免 USB2 頻寬不足)以符合 srsLTE 的基本系統要求。

RF 硬體 ： USRPs

- USRP B210 軟體定義無線電開發板 2 片
- USB3 連接線 2 條
- VERT900 Antenna (824-960 and 1710-1990 MHz) Dualband 4 根
- VERT2450 Antenna (2.4-2.5 and 4.9-5.9 GHz) Dualband 4 根

SIM 卡 ：

- T-STAR(台灣之星) 的 USIM 1 張

使用者端設備(UEs) ：

- ASUS Zenfone 6(2019) 執行 Android 10.0 1 台
- ASUS Zenfone 3 執行 Android 9.0 1 台
  兩台皆支援 4G LTE 網路通訊。

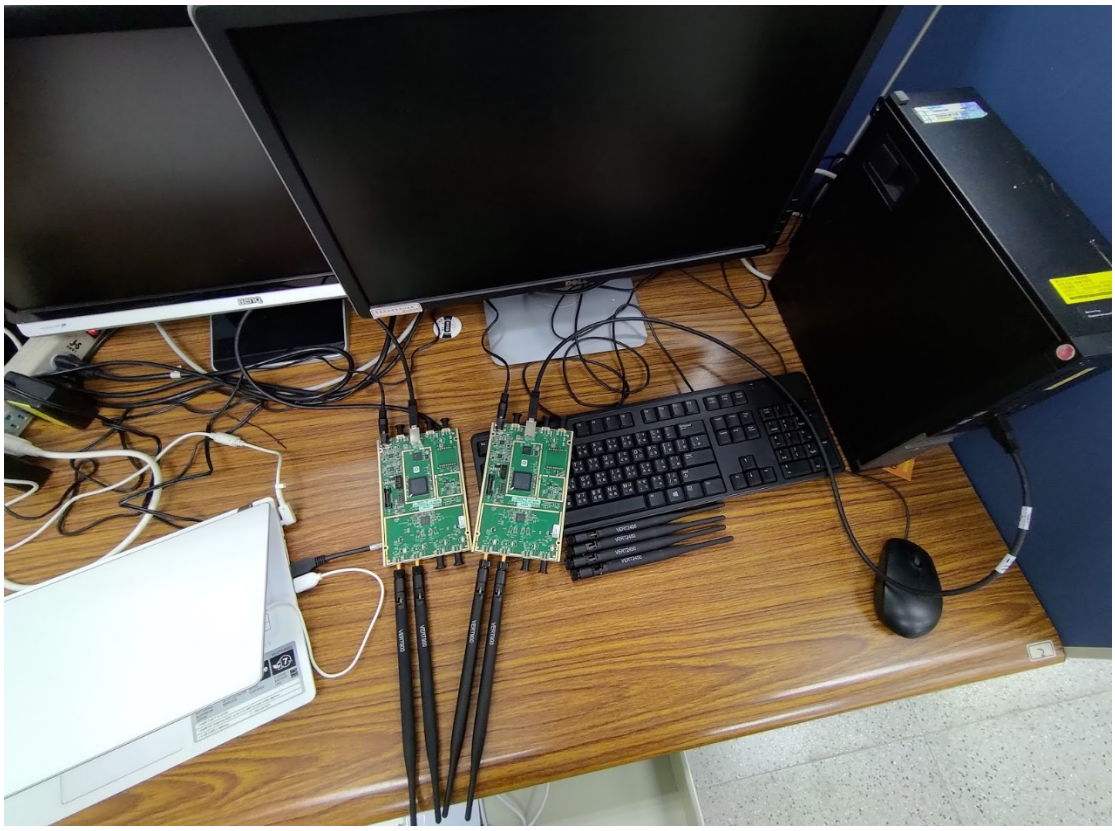


圖 3 實驗設備(不包含 UE)

軟體 ：

- UHD (USRP Hardware Driver) : USRP 設備的驅動程式[2]

- srsLTE 19.12： 由 Software Radio Systems (SRS)公司開發的免費開源 LTE SDR 套裝平台。[1]
- Wooniety/srsLTE-Sniffer： 參考其程式碼，引用部份功能解析 ASN-1 代碼。[8]
- WireShark： 網路封包分析軟體，用來讀取與分析 pcap 檔案。
- LTE Discovery[14] : Android 平台上的訊號分析 APP，支援 3G GSM, 4G LTE, 5G NR 之訊號分析。
- Service/Testing Mode： 大部分手機作業系統都有內建測試模式，其提供使用者一般無法存取的手機裝置與目前的無線通訊狀態之資訊。以我們的裝置為例，在撥號程式輸入*#*#4636#*#*，即可進入「手機資訊」頁面。我們可以得到 IMSI 等有用資訊。

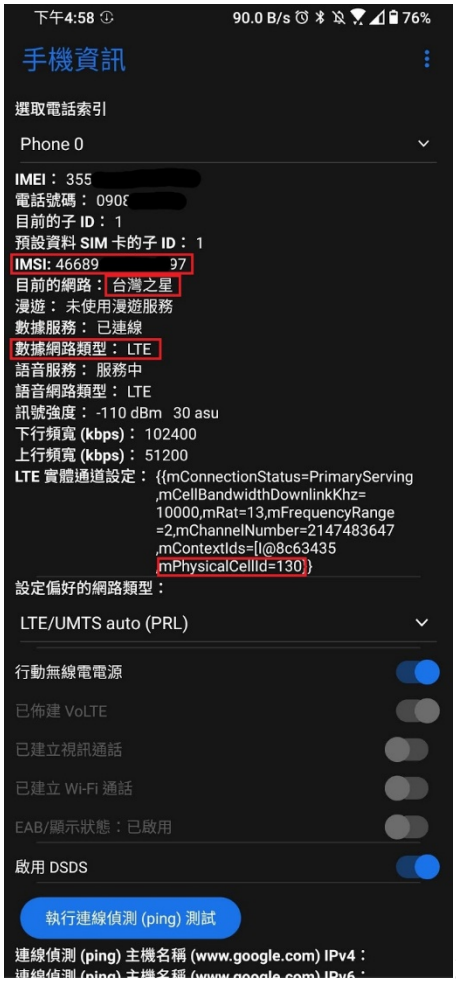


圖 4 Testing Mode 的「手機資訊」 (Android)

4. LTE 探聽工具設計

我們探聽工具的設計架構，主要分三個階段：

第一階段：進行基地台搜尋，了解周遭基地台與頻帶分布狀況[11]，並且得到各基地台 EARFCN，用以鎖定後續的探聽目標。

第二階段：指定頻帶，透過擷取目標基地台廣播的 MIB(Master Infomation Block)、SIB 封包，取得基地台相關參數(PLMN、TAC)，以便後續測量與設置假基地台使用。

第三階段：我們利用兩種方式進行攻擊，第一種是持續探聽 Paging Records，屬於被動式的手段，透過探聽傳呼紀錄的 s-TMSI 資料，可以整理出附近 UE 的資訊，利用其配合 TAC 分析地點進行定位。

另一種是主動式的模擬假基地台，透過代入上面獲得的參數，我們可以騙取 UE 嘗試連線，從連線建立過程中，取得 UE 的 IMSI，並透過 Service Reject 其請求，達到類似 DoS 攻擊的效果，干擾 UE 的正常連線。

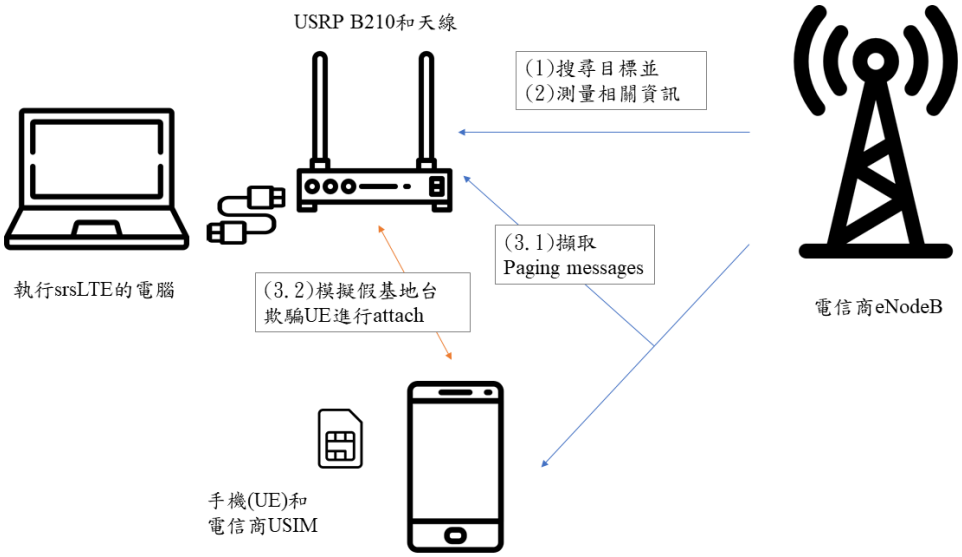


圖 5 LTE 探聽工具的設計架構

5. 實驗過程與結果

在本節中，我們承上述之設計架構，改造開源程式碼，實際進行探聽工具的架設，並觀察結果。

5.1. 基地台搜索

使用 srsLTE 的範例程式 cell_search，使用 USRP B210 與不同頻率增益的天線，掃描常用頻段，找尋附近的基地台訊號，並整理結果用以選擇可能的目標。

表格 1 搜尋鄰近基地台之結果

PCI (Physical Cell ID)	電信商	頻段 (Band)	DL-EARFCN	主同步訊號 (Primary Synchronization Signal, PSS) 功率

316	CHT	Band 3	1400	-33.7dBm
316	CHT	Band 8	3650	-33.8dBm
130	T-STAR	Band 8	3550	-33.4dBm
312	TWM	Band 28	9560	-25.9dBm

並在使用台灣之星 USIM 的手機(Zenfone6)上使用 LTE Discovery 程式，檢查手機的連線資訊，我們想以台灣之星(T-STAR)的基地台作為目標。

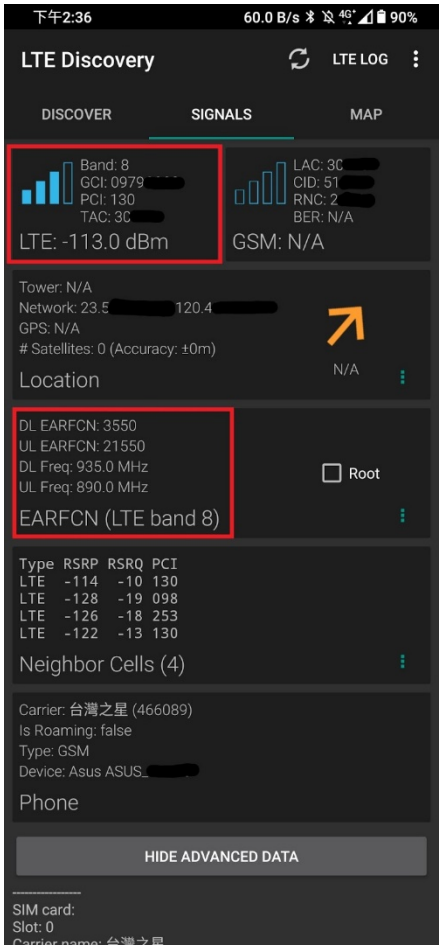


圖 6 LTE Discovery 顯示之手機連線資訊

我們選擇手機連線到的 Band8 的 T-STAR 基地台，PCI=130，DL-EARFCN = 3550 為目標做後續的測量與探聽。

5.2. 廣播封包探聽

透過修改 srsLTE 內的 pdsch_ue 程式碼以及 srsUE 的設定，並指定目標頻率，我們可以解析目標基地台所廣播之 MIB、SIBs 的資料。

```
  - Type:             FDD
  - PCI:              130 #Physical Cell ID
  - Nof ports:        2
  - CP:               Normal
  - PRB:              50
  - PHICH Length:     Normal
  - PHICH Resources: 1/6
  - SFN:              217
Decoded MIB. SFN: 217, offset: 0
```

圖 7 解碼之 MIB 資訊

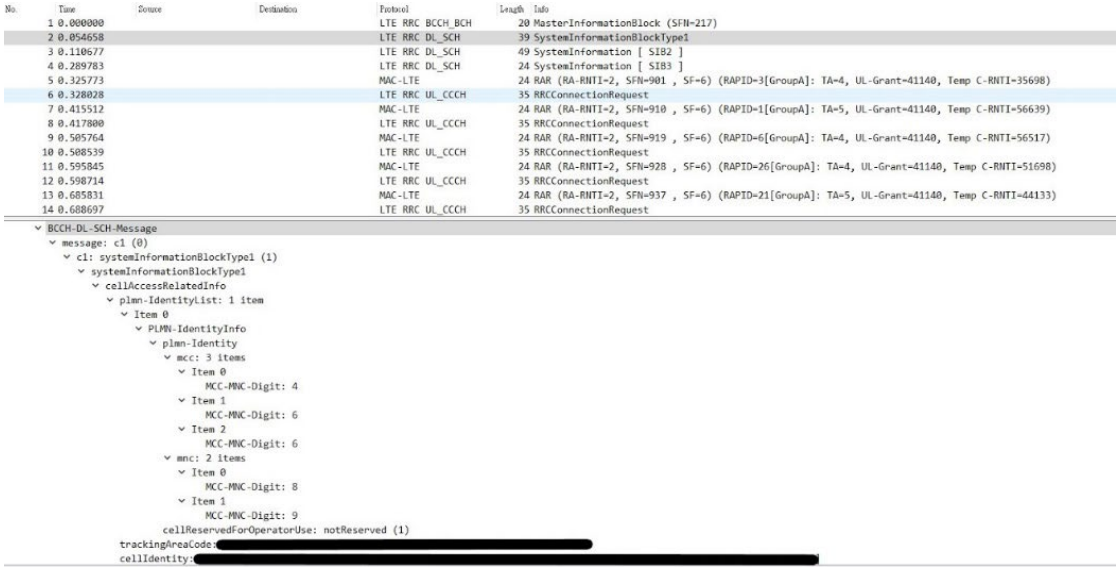
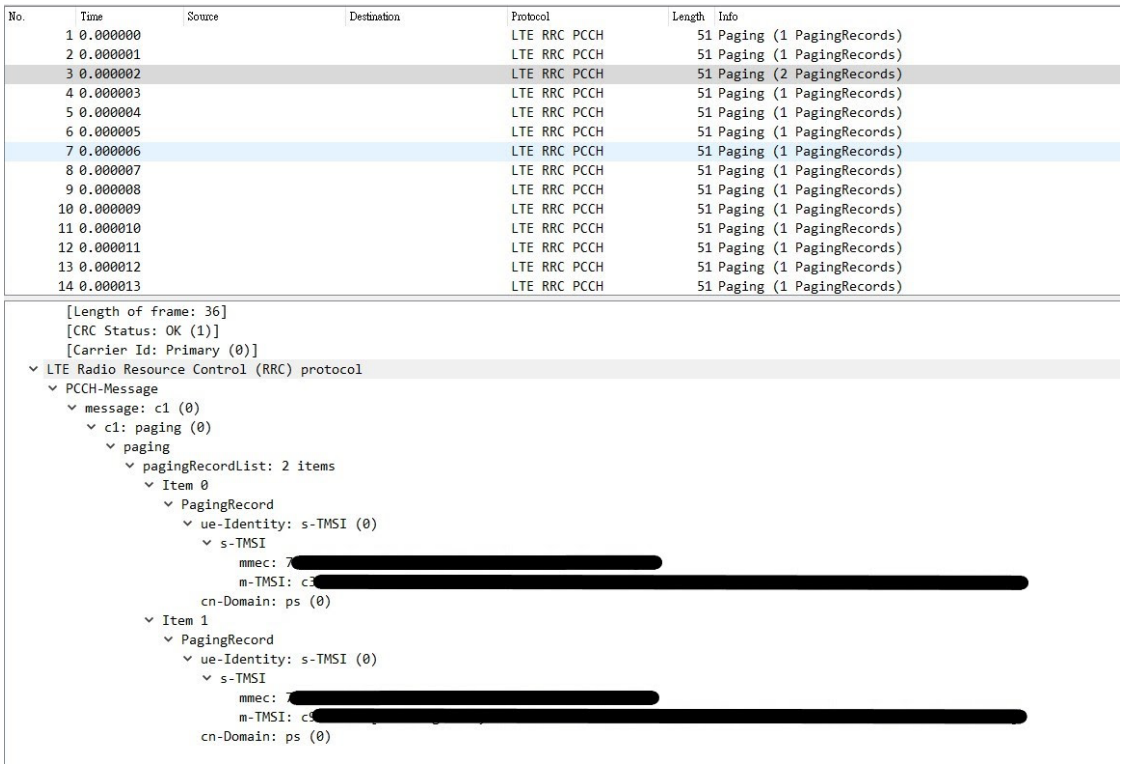


圖 8 透過 WireShark 檢視 srsUE 所抓取到之 SIB 封包

我們關注的是 MCC、MNC 與 TAC 這些與基地台選取有關的參數。

5. 3. 探聽 Paging Records 與模擬假基地台

再度執行上述修改的 pdsch_ue，這次指定其探聽 RNTI=0xfffe 之封包[15]，並且參考 Wooniety/srsLTE-Sniffer[9]之程式碼，將 Paging Records 原始的位元組轉譯為 pcap 封包擷取檔，以 WireShark 讀取。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			LTE RRC PCCH	51	Paging (1 PagingRecords)
2	0.000001			LTE RRC PCCH	51	Paging (1 PagingRecords)
3	0.000002			LTE RRC PCCH	51	Paging (2 PagingRecords)
4	0.000003			LTE RRC PCCH	51	Paging (1 PagingRecords)
5	0.000004			LTE RRC PCCH	51	Paging (1 PagingRecords)
6	0.000005			LTE RRC PCCH	51	Paging (1 PagingRecords)
7	0.000006			LTE RRC PCCH	51	Paging (1 PagingRecords)
8	0.000007			LTE RRC PCCH	51	Paging (1 PagingRecords)
9	0.000008			LTE RRC PCCH	51	Paging (1 PagingRecords)
10	0.000009			LTE RRC PCCH	51	Paging (1 PagingRecords)
11	0.000010			LTE RRC PCCH	51	Paging (1 PagingRecords)
12	0.000011			LTE RRC PCCH	51	Paging (1 PagingRecords)
13	0.000012			LTE RRC PCCH	51	Paging (1 PagingRecords)
14	0.000013			LTE RRC PCCH	51	Paging (1 PagingRecords)

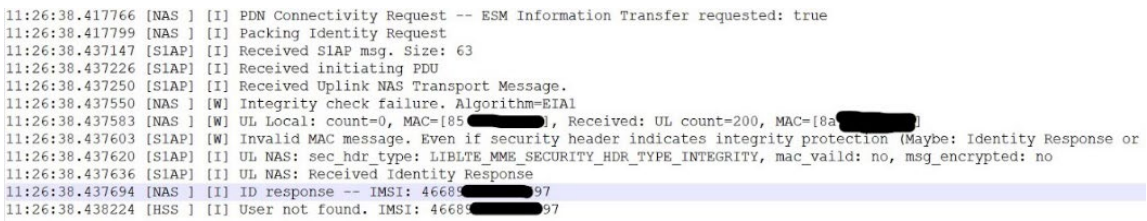
圖 9 透過 WireShark 檢視抓取之 Paging Messages

我們可以看到其 Paging Record 包含 UE 的 s-TMSI 身分資料。

接下來我們試著進行主動式的攻擊，利用上面測量到的參數，設定 srsLTE 建立假基地台。

我們模擬假基地台偽裝為目標基地台，使用一樣的 DL-EARFCN 頻率，設定一樣的 PLMN 與 TAC。

在 UE 進行重選時，會嘗試與假基地台進行連線，因為 UE 信任其為合適的基地台，而且基地台向其請求身份資訊。



```
11:26:38.417766 [NAS ] [I] PDN Connectivity Request -- ESM Information Transfer requested: true
11:26:38.417799 [NAS ] [I] Packing Identity Request
11:26:38.437147 [S1AP] [I] Received S1AP msg. Size: 63
11:26:38.437226 [S1AP] [I] Received initiating PDU
11:26:38.437250 [S1AP] [I] Received Uplink NAS Transport Message.
11:26:38.437550 [NAS ] [W] Integrity check failure. Algorithm=EIA1
11:26:38.437583 [NAS ] [W] UL Local: count=0, MAC=[85[redacted], Received: UL count=200, MAC=[8a[redacted]
11:26:38.437603 [S1AP] [W] Invalid MAC message. Even if security header indicates integrity protection (Maybe: Identity Response or
11:26:38.437620 [S1AP] [I] UL NAS: sec_hdr_type: LIBLTE_MME_SECURITY_HDR_TYPE_INTEGRITY, mac_vaild: no, msg_encrypted: no
11:26:38.437636 [S1AP] [I] UL NAS: Received Identity Response
11:26:38.437694 [NAS ] [I] ID response -- IMSI: 46689[redacted]97
11:26:38.438224 [HSS ] [I] User not found. IMSI: 46689[redacted]97
```

圖 10 捕捉到之 IMSI

我們透過 ID Response 收集到了 UE 的 IMSI 資訊，不過因為我們的 HSS Database 沒有認證的密鑰，NAS 服務會 Service reject (Implict Detatched)，無法完成連線。

若是 UE 所在位置剛好搜尋不到更合適的基地台，多次嘗試未果後，會認為無法連線，顯示沒有服務，間接造成類似 DoS 的效果。

6. 結論

我們的專題證明了，低成本的 LTE IMSI-Catching 攻擊/干擾裝置是可行的。我們展示了(1)可以透過簡易的 SDR 設備自製 LTE 搜尋裝置，快速掃瞄，並收集附近基地台資訊。(2)透過模擬假基地台，LTE 的連線會被干擾，並可能洩漏隱私。

而且透過開源軟體，其所需要的程式門檻也變得較低，因此更容易被有心人士利用，對商用行動網路造成影響。我們希望這個專題以及其他人的研究，能讓電信服務提供商注意到這個問題，即便現在國內 5G NR 已經商轉的情況下，大部分人仍然在使用 4G LTE 網路，不能保證日後都不會受到影響。希望未來能夠繼續改善行動網路協定的安全性與隱私權，以因應日漸增加的需求。

致謝

感謝碩士生 吳柏諺，協助設備管理與提供格式修正建議。

感謝碩士生 劉君泰，提供用詞與格式修正建議。

圖 5 之素材，取自 https://www.flaticon.com/free-icon/。

參考文獻

[1] srsLTE - Open-source LTE software radio suite developed by Software Radio Systems (SRS). https://www.srslte.com/

[2] Ettus Research - The leader in Software Defined Radio(SDR). https://www.ettus.com/

[3] Stig F. Mjølsnes and Ruxandra F. Olimid,"Easy 4G/LTE IMSI Catchers for Non-Programmers", 2017. https://arxiv.org/pdf/1702.04434.pdf

[4] Christian Sørseth · Xianyu Shelley Zhou · Stig F. Mjølsnes ·Ruxandra F. Olimid,"Experimental Analysis of Subscribers' Privacy Exposure by LTE Paging", 2018 https://arxiv.org/pdf/1807.11350.pdf

[5] Teng Fei and Wenye Wang,"LTE is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks", In 2019 IEEE Global Communications Conference, 2019. https://research.ece.ncsu.edu/netwis/papers/19FW-GB.pdf

[6] Altaf Shaik , Ravishankar Borgaonkar , N. Asokan , Valtteri Niemi and Jean-Pierre Seifert,"Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems",2016. https://arxiv.org/pdf/1510.07563v2.pdf

[7] Roger Piqueras Jover,"EXPLORING LTE SECURITY AND PROTOCOL EXPLOITS WITH OPEN SOURCE SOFTWARE AND LOW-COST SOFTWARE RADIO" ,2016. http://rogerpiquerasjover.net/LTE_open_source_HackerHalted.pdf

[8] Adam Toscher,"How to create an EVIL LTE Twin",2019. https://medium.com/@adam.toscher/how-to-create-an-evil-lte-twin-34b0a9ce193b

[9] Wooniety/srsLTE-Sniffer https://github.com/Wooniety/srsLTE-Sniffer

[10] NCC 國家通訊傳播委員會 – 行動網路識別碼核配現況.
https://www.ncc.gov.tw/chinese/files/14050/%e8%a1%8c%e5%8b%95%e7%b6%b2%e8%b7%af%e8%ad%98%e5%88%a5%e7%a2%bc%e6%a0%b8%e9%85%8d%e7%8f%be%e6%b3%81.pdf
[11] NCC 國家通訊傳播委員會–頻率資料庫查詢系統. https://freqdbo.ncc.gov.tw/portal/index.aspx
[12] ETSI TS 136 331 V13.0.0 (2016-01): LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (3GPP TS 36.331 version 13.0.0 Release 13) , 2016.
http://www.etsi.org/deliver/etsi_ts/136300_136399/136331/13.00.00_60/ts_136331v130000p.pdf
[13] LTE and Wireless Study : Paging Process.
http://xdxdd.blogspot.com/2012/08/lte-paging-proccess.html
[14] LTE Discovery On Google Play.
https://play.google.com/store/apps/details?id=net.simplyadvanced.ltediscovery
[15] LTE Quick Reference - RNTI.
https://www.sharetechnote.com/html/Handbook_LTE_RNTI.html#TypeOfRNTI