Don’t Shoot the Messenger! ~ Localization Prevention of Satellite Internet Users

出處: David Koisser, Richard Mitev, Marco Chilese, Ahmad-Reza Sadeghi,
Cornell University, 2024 IEEE Symposium on Security and Privacy (SP)

成員: B113040002 林之謙、B113040029 曾柏諺

零、大綱

本文將先會先介紹這篇論文所要改善的核心技術 — 衛星上網，以及筆者團隊的研究動機、所要解決的問題，以及目前遇到的困難。還會介紹目前在聯網相關的防護機制以及他們為何無法防範攻擊者的攻擊。隨後會介紹團隊所構想的模型以及實驗限制，並且介紹他們為了解決各個懸念而設計的一些小巧思。

再來會介紹他們的實驗進行方式以及得到的數據，最後是分享我們自己建立的全軟體簡易復刻模型，其中包含了前面章節提到的一些機制以及

壹、什麼是衛星上網

衛星上網是一種新的形態的網路系統，他將原本跨海的傳輸部分由海底電纜改成用低軌衛星幫忙傳輸。使用這會從客戶端用傳統的本地網路連線到 Gateway，再由 Gateway 幫忙將訊號以雷達電波的形式上鏈(uplink) 到衛星，再由衛星下鏈 (downlink) 給遠端的網路中心進行服務。回程也是相同的模式進行。雖然現行的衛星上網在使用體驗上仍不及傳統網路系統，但其所展示的可能性能使線纜索無法到達的偏遠地區，甚至是海中央也能夠進行通訊。

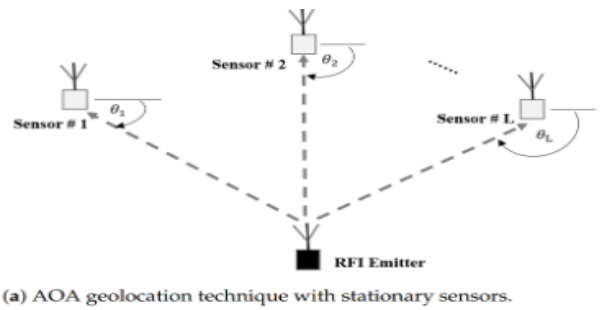
烏俄戰爭中，Starlink 免費為烏克蘭提供了衛星上網的服務，這使得烏克蘭人民在戰火摧殘下也能和外界進行聯繫。然而這同時也催生出一個問題，那就是上下鏈的衛星訊號是否有可能被敵軍用來定位暗殺目標? 歷史上確實有不少記者因為向外界轉播實況而被盯上。在人手一機，所有人都能時實轉播戰況的狀況下，有心人士可以利用三角定位鎖定目標位置。**研究團隊的目的就在於防止使用者的位置因上鏈的 Gateway 被定位而曝光。**

貳、攻擊者如何鎖定目標位置

攻擊者可以利用三角定位法鎖定目標位置，目前常見的方法有三種 :

1. **AOA (Angle-of-arrival) :**
   由於衛星訊號並非點對點，而是發散的訊號，因此攻擊者可以利用訊號對衛星的入射角來算出期和基站的直線公式，並反推其位置，只要至少兩顆衛星就可找出目標基站的位置。

$$\theta_i = tan^{-1}\left[\frac{(y - y_i)}{(x - x_i)}\right]$$



(a) AOA geolocation technique with stationary sensors.

▲ AOA 的情境示意圖

2. **TOA (Time-of-Arrival)**
   此法利用訊號到達衛星的時間推算出其距離，需要至少三顆衛星推算距離後再各自以衛星為圓心畫圓。此三個圓周之交點就是 uplink gateway 之所在。

$$\tau_i = \frac{d_i}{c}$$

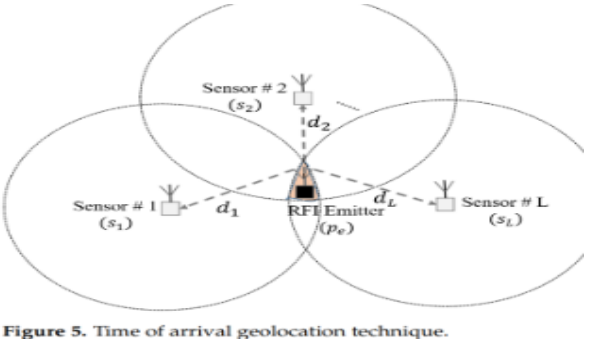
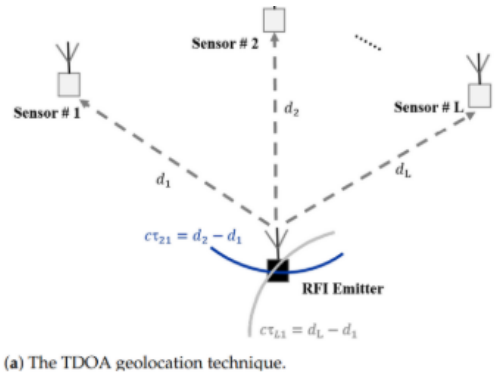


Figure 5. Time of arrival geolocation technique.

▲ **TOA** 的情境示意圖

3. **TDOA (Time-Difference-of-Arrival)**
   和 TOA 不同，這個方法是監測信號到達兩個衛星的時間差，求得雙曲線函數再線性化並用LS估計正確位置。可以使用三顆以上的衛星監測。

$$\tau_{i1} = \frac{(d_i - d_1)}{c},$$



(a) The TDOA geolocation technique.

▲ **TDOA** 的情境示意圖

4. **FDOA (Frequency-Difference-of-Arrival)**
   和 TDOA 相似，但這個方法是監測信號到達兩個衛星的信號頻率的都卜勒校位移，求得雙曲線函數再線性化估計正確位置。同樣可以使用三顆以上的衛星。也有和 TDOA 混合使用的種類。

$$\partial f = v\left(\frac{f_0}{c}\right) \qquad \text{FDOA} = f_{i1} = \partial f_i - \partial f_1$$

以上三角定位法皆沒有要求解密電波訊息，單純只要電波本身難以隱藏的物理性質(入射角、頻率、相位、timestamp、來源位置) 即可鎖定地面的基站位置。同時波還具備「廣播性」，使得他的訊息很容易被目標附近的裝置監聽。最後是因為衛星上網的系通需要對波進行訊息修正，因此其電波必含有不得隱藏的前導序列訊息，這也是難以對攻擊者隱藏的訊息。因此衛星上網的定位追蹤才被視為難處理的問題。

參、傳統技術為何無法幫助匿名

論文中提出了三個傳統技術作為參考，分別是TLS/HTTPS、VPN、與Tor。

TLS的設計目的本來就只是對傳輸的資訊本身進行加密，而隱藏資訊的傳輸路徑和傳送者的地理位置則不在考慮範圍內。

VPN確實是會隱藏IP，但那是在抵達VPN伺服器，也就是已經送出衛星之後了。而我們想要隱藏的上傳路徑仍然會被觀測到。

Tor雖然可以完美的達成我們的需求，但他有一個大前提，就是出入口不能被掌控。然而在論文預設的前提下，衛星這個唯一的出入口是很容易被監控的。

伍、實驗模型

研究團隊為了解決這個問題提出了 AnonSat 系統。不同於對訊號進行處理，他們選擇向「隱藏真實位置」的方面出手。

AnonSat 會用一定範圍內的 Gateway 組成本地網路，再讓使用者 routing 到其他 Gateway 進行上鏈，如此即使該上鏈 Gateway 的位置曝光也不會被查出使用者的真實位置。

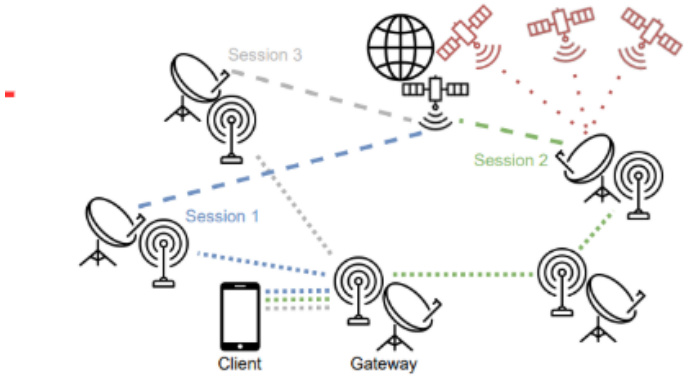


Figure 1. An example setup of AnonSat with five gateways and one client.

▲ AnonSat 的示意圖

他們的實驗是模仿烏俄戰爭的狀況，因此實驗模型存在一些前提假設:

- 攻擊者：
  1. 具有一組用於監聽的衛星
  2. 可以攔截Gateway間的通訊
  3. 無法攔截 client 到自己的 Gateway間的通訊
  4. 但不具監控整個 local network 的能力
  5. 無法破譯 Gateway 間的 per-hop 簽章

- 模型：
  1. 戰場上傳統上網方式已經失效，只剩衛星上網能運作
  2. 衛星無法取的本地網路內流通的無線電波
  3. Gateway 間用憑證和對稱密鑰 驗證彼此

在這樣的情境下，研究團隊在設計 AnonSat 上有四個目標要達成：

R.1 防止基站地理定位 — 防止攻擊者衛星掌握客戶地理位置
R.2 防止本地網路資訊洩漏 — 防止攻擊者竊聽部分本地網路通訊找出客戶位置

R.3 和既有網際網路服務相容 **—** 可以直接兼容已有的網路服務不須額外做調整
R.4 Out-of-the-box — 可以直接使用，不必下載額外資源或做更多調整

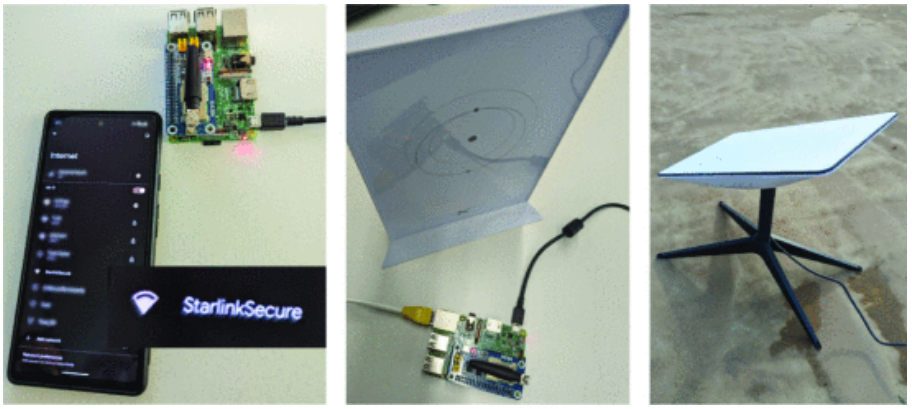
首先針對 R2 的要求，團隊新增了 Per-hop encryption 以及 Gateway timeout，前者是讓每對 Gateway 間維持一個暫時性的共同密鑰，並僅在此兩點通訊時使用，forward 到下一個 Gateway 時會改用和該點協商出的密鑰。如此可以防止攻擊者透過監聽特定段的傳輸破解 routing 的資訊，以此找出客戶所在。而後者則是設置一個連線 Timer 防止連線時間過而讓攻擊者可以根據路由路徑逆向追蹤客戶所在的源頭。每當這個 Timer 發生 timeout，會重新選擇另一個 Gateway 當做 Uplink Gateway 並重新做 routing。

針對 R1，則是有「偏好方向」的設計。一般來說，如果環境中的 Gateway 都平均分散，那當多次聯網後選擇過的 Uplink Gateway 就有可能以客戶為圓心呈現輻射狀分布，如此一來衛星就可以用數學方法算出客戶所在的 Gateway。因此如果在選擇Uplink Gateway 時讓特定方項的 Gateway 更容易被選上，那就能使客戶不會在所有 Uplink Gateway 的中心，也就無法算出客戶位置。

除了上述之外，研究團隊還定了 Max_ hops 來控制路徑的跳數，因為如果路徑太短，Uplink Gateway 可能和客戶端相近，從而喪失從其他 Gateway 上鏈的意義，太長則會讓花在本地網路的時間增加，造成連線效率變差。因此須經測驗後決定數值。

陸、研究團隊模型

團隊實作的模型為了驗證這個模型不需要使用特製的裝置來達成，所有的裝置都是採用市售品。為了模擬衛星網路通訊的狀況，他們採用了SpaceX的starlink服務來模擬從天線透過衛星傳送資料，用Raspberry Pi的主板搭載semtech的sub-GHz LoRa SX1262通訊擴充板來模擬地面站，最後用Android手機來模擬正常人用衛星上網的行為。



論文團隊還評估過使用SX1280這個比較新的板子，但是官方提供的驅動程式導致每次傳送封包還有50ms的延遲，進而讓有效數據率低於SX1262。加上SX1262有比較完整的套件可以和Raspberry Pi主板進行結合。

接著是通訊的頻道。論文中選擇的是868Mz。主要理由便是這個頻道為免執照頻段，不需要進行額外的申請。此外，低頻可以使其有更高的傳播距離和穿透力。686 MHz也較少被占用，干擾較少。

再來是軟體層面，團隊使用了github上一個叫做tncattach的專案，將IP傳送的封包整合成LoRa所需要的格式，另外，因為tncattach不支援一次性傳送超過236bytes的封包，團隊額外寫了切分並編號封包的程式。

柒、實驗結果和匿名性評估

首先，作為測試跳躍數對封包的傳輸時間和掉包機率的影響，團隊針對0跳(所連接的WiFi基地台直連衛星)、1跳(WiFi基地台接收封包後轉傳給另一個基地台上衛星)跟2跳(中間再多一個中繼基地台)進行100次的64bytes的ICMP echo request，並監測往返時間與未收到的reply數量來計算結果。然而這個測試沒有使用到前面提到的切分封包的功能，所以這個測試只能做為參考。結果如下圖：

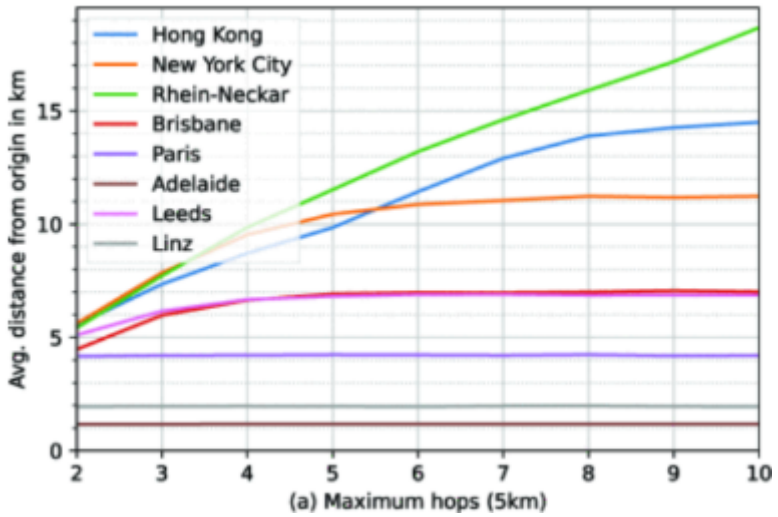
LoRa Hops	RTT	Packet Loss
0	49.111 ms	0%
1	157.938 ms	3%
2	211.786 ms	4%

接著，團隊測試了傳送不同大小的壓縮圖片。環境上是選用2跳，使用時間如下圖。另外，雖然論文未提供掉包率，但從文中提到有明顯的重傳現象可以推測掉包率不算低。

Image Size	Upload	Download
50 kB	65.84 s	60.40 s
100 kB	137.84 s	117.80 s
150 kB	171.92 s	223.20 s
200 kB	269.31 s	276.80 s

後續，他們接連測算了不同跳躍數平均能離開使用者多遠，以及在不同的網路技術下使用網路服務時交換協議的用時與資料傳輸速率。結果如下：

1. 每一跳採用五公里內任意節點下的平均距離：
   max_hops = 1 → 平均距離 ≈ 3 km
   max_hops = 3 → 平均距離 ≈ 8 km
   max_hops = 5 → 平均距離 ≈ 12 km



上圖的橫軸為最大跳數，縱軸為離原地點距離。可推斷節點越密集距離越短。

2. TLS交換協議用時(影響用戶上網前的等待時間)如下表：

網路類型	節點數	平均握手延遲 (ms)	峰值延遲 (ms)
LoRa 5 km @50 kbps	10	420	600
LoRa 5 km @50 kbps	50	800	1200
DASH7 5 km @166 kbps	10	250	350
DASH7 5 km @166 kbps	50	450	650
LoRa2.4/ LTE-M1 1 km	10	150	200
LoRa2.4/ LTE-M1 1 km	50	300	450
LTE-M2 1 km @4 Mbps	10	120	160
LTE-M2 1 km @4 Mbps	50	180	240

3. 上傳200kB圖片所需時間(用於資料傳輸效率的測試):

網路類型	節點數	上傳**200kB**圖片平均時間 (秒)
LoRa 5 km @50 kbps	10	170
LoRa 5 km @50 kbps	50	330
DASH7 5 km @166 kbps	10	90
DASH7 5 km @166 kbps	50	160
LoRa2.4/LTE-M1 1 km	10	35
LoRa2.4/LTE-M1 1 km	50	60
LTE-M2 1 km @4 Mbps	10	10
LTE-M2 1 km @4 Mbps	50	18

匿名性評估:

因為論文團隊並沒有實際的測試在攻擊之下用此方法的匿名能力，所以只能使用數據去推估匿名性。團隊採用了方式是去計算匿名集，也就是在攻擊者透過gateway去尋找來源時，有多少可能的gateway。然後再根據其他資訊進一步推算出實際上在攻擊時的gateway可能。

另外，文章中還有去算這個系統的抗攻擊能力，也就是這個系統在AB兩個節點之間，有多少種不同的路徑(不計入會重複經過相同節點的路徑)。這個數據可以反映特定節點被攻陷後是否能有其他可用路徑。

匿名性的相關數據被團隊整理成下表:

	5 km Average Anonymity Set	5 km Minimum Anonymity Set	5 km Average Effective Set	5 km Minimum Effective Set	5 km Average Node2node Paths	5 km Average Unique Paths	1 km Average Anonymity Set	1 km Minimum Anonymity Set	1 km Average Effective Set	1 km Minimum Effective Set	1 km Average Node2node Paths	1 km Average Unique Paths
Hong Kong	417.3	12	278.0	9.1	6 080.3	54.2	111.8	26	60.1	21.8	5 147.9	5.7
New York City	523.7	13	330.0	12.6	6 415.1	59.9	92.7	8	47.7	8.0	3 734.4	4.2
Rhein-Neckar	98.5	11	60.4	7.5	193.1	8.9	18.3	13	12.2	9.1	116.2	2.3
Brisbane	83.7	17	61.9	14.9	862.9	20.2	35.3	30	26.7	20.8	116.5	4.3
Paris	180.0	179	172.7	162.4	10 096.9	93.8	78.4	12	43.0	9.4	332.2	2.7
Adelaide	50.0	50	50.0	50.0	2 402.0	50.0	50.0	50	44.7	43.7	2 045.5	13.4
Leeds	149.7	49	121.4	39.5	1 880.1	35.6	37.9	10	22.5	8.4	61.2	2.1
Linz	33.0	33	33.0	33.0	959.8	31.6	37.9	26	20.7	19.2	834.3	4.6

捌、我們的實作

平台: WSL (ubuntu 24.0.1)

我們的實作內容是嘗試自己用全軟體的方式模擬第陸節的實驗模型，但因論文並沒有提供任何資源，故此模型的功能全部由我們自行推敲，難免會有先簡陋。

首先我們需要建立虛擬節點來做連線，因此我們使用 Mininet 來建立網路拓樸。Mininet 是一個 Linux 用的Python套件，Mininet 能夠設立許多節點並指定 host、switch、router、server 等角色給它們，並使其彼此間建立連線以此建立本地網路的網路拓樸。使用者也可以用來運行自己寫的SDN等程式。Mininet 的 shell 也擁有些許命令可以查看拓樸資料或是測試效能。

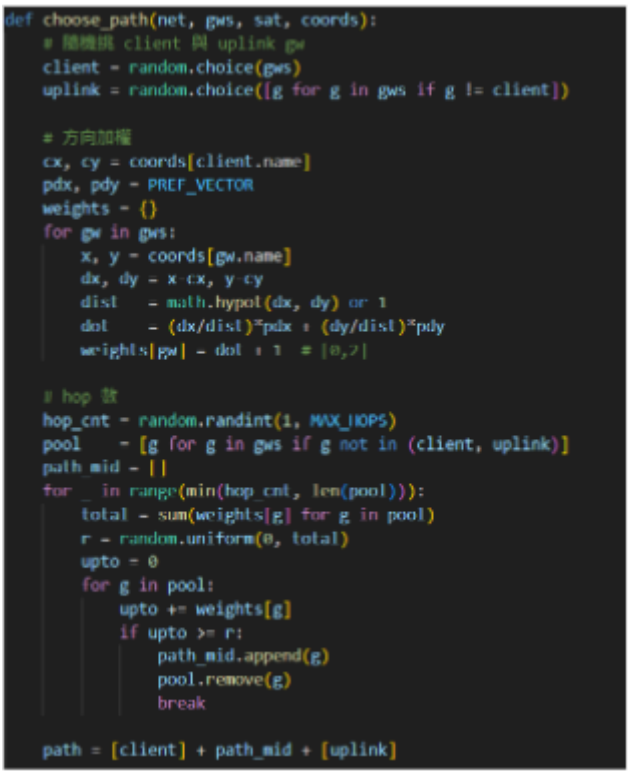
再來我們利用 NetEm 來模擬低軌衛星低延遲、高頻寬的傳輸特徵。

我們的模型運作主要分為兩個階段，收先會宣告出指定數量的節點，然後使所有節點兩兩相聯，形成 Full Connection 的本地網路，再從中選擇這次的客戶位置。

接下來每個會將 Max_hops 和 偏好方向納入考量，選出這次的 uplink target 並排出路由路徑。此路徑會用套件的 command 計算一次 RTT，如果這次路由的時間比RTT還要久，則會捨棄當前路徑，重新做一次路由。

```python
def build_topo():
    net = Mininet(link=TCLink, controller=None)

    # sat host
    sat = net.addHost('sat', ip='10.0.255.2/24')   # 固定

    # nodes
    gws  = [net.addHost(f'gw{i}') for i in range(1, GATEWAY_COUNT+1)]

    # Build full connection between nodes
    for i in range(GATEWAY_COUNT):
        for j in range(i+1, GATEWAY_COUNT):
            net.addLink(gws[i], gws[j], cls=TCLink)

    net.addLink(gws[0], sat, cls=TCLink,
                delay='60ms', loss=0.1, bw=100, use_hfsc=True)
```

▲ 宣告節點並建立連線



```python
def choose_path(net, gws, sat, coords):
    # 隨機挑 client 與 uplink gw
    client = random.choice(gws)
    uplink = random.choice([g for g in gws if g != client])

    # 方向加權
    cx, cy = coords[client.name]
    pdx, pdy = PREF_VECTOR
    weights = {}
    for gw in gws:
        x, y = coords[gw.name]
        dx, dy = x-cx, y-cy
        dist   = math.hypot(dx, dy) or 1
        dot    = (dx/dist)*pdx + (dy/dist)*pdy
        weights[gw] = dot + 1  # [0,2]

    # hop 數
    hop_cnt = random.randint(1, MAX_HOPS)
    pool    = [g for g in gws if g not in (client, uplink)]
    path_mid = []
    for _ in range(min(hop_cnt, len(pool))):
        total = sum(weights[g] for g in pool)
        r = random.uniform(0, total)
        upto = 0
        for g in pool:
            upto += weights[g]
            if upto >= r:
                path_mid.append(g)
                pool.remove(g)
                break

    path = [client] + path_mid + [uplink]
```

▲ 執行 **routing**

接下來要介紹我們實作出的三特殊機制:

1. 偏好方向:
   首先會決定一個常數二座標作為偏好方向向量，而後再將 client 到所有點的向量和該常數向量算內積。回傳出來的值即是之後用於選擇 router 的權重值。

```python
PREF_VECTOR    = (1, 0)
```

```python
# 方向加權
cx, cy = coords[client.name]
pdx, pdy = PREF_VECTOR
weights = {}
for gw in gws:
    x, y = coords[gw.name]
    dx, dy = x-cx, y-cy
    dist   = math.hypot(dx, dy) or 1
    dot    = (dx/dist)*pdx + (dy/dist)*pdy
    weights[gw] = dot + 1  # [0,2]
```

▲ 計算每個點的偏好加權

2. 建立路經:
   選擇完 uplink Gateway 後，程式會加總每個點的權重值，然後隨機選擇一個該值範圍內的數值。再次重 0 開始加總權重，如果某次加完後的總合大於等於隨機值，則表示這次會選擇此點作為 next hop。

```python
# 建立路徑
hop_cnt = random.randint(1, MAX_HOPS)
pool    = [g for g in gws if g not in (client, uplink)]
path_mid = []
for _ in range(min(hop_cnt, len(pool))):
    total = sum(weights[g] for g in pool)
    r = random.uniform(0, total)
    upto = 0
    for g in pool:
        upto += weights[g]
        if upto >= r:
            path_mid.append(g)
            pool.remove(g)
            break

path = [client] + path_mid + [uplink]
```

▲ 建立這次 **route**

3. **Timeout:**
   產生 route 之後會立即用系統指令測試此 route 的 RTT，如果此 RTT 超過設定的 Timeout Interval 則會要求重新選擇 Uplink Gateway 並 routing。

```python
# RTT 測試
def measure_rtt(client, sat):
    sat.cmd('pkill -f \"http.server\" || true')
    sat.cmd('python3 -m http.server 8000 &')
    time.sleep(0.5)
    out = client.cmd(f'timeout {TIMEOUT}s curl -s --fail http://10.0.10.2:8000')
    return bool(out.strip())

if __name__ == '__main__':
    setLogLevel('info')
    net, gws, sat, coords, client = build_topo()

    while True:
        client, sat_host = choose_path(net, gws, sat, coords, client)
        if measure_rtt(client, sat_host):
            print('Connection succeed\nEntering CLI。')
            break
        else:
            print(f'TIMEOUT={TIMEOUT}s Rerouting…')
```

▲ 利用指令重新計算 **RTT**

玖、實作項目的缺點

我們的實作內容有機個明顯的缺點，首先他只是個簡易的改念模型，因此無法處理太大規模的情境。Mininet 並非為了大規模情境設計的，他一次能處理的節點數和本機的硬體條件有絕對關係，故我們的模型無法一次宣告上百的節點以模仿真實情境。

Mininet 也無法模擬真實的地理條件，因此我們的模型並沒有含納這一部份的考量，其中僅有的 2D 座標也是我為了實現偏好方向追加的，而這已經是我們能想到的最好的地理位置模仿了，但物理距離對兩點間傳輸時長的影響這支程式卻無法再現。

最後是攻擊型態的模擬，我們不知道要怎麼模擬攻擊者衛星的行為模式和攻擊方法，使得我們只能藉由運行結果揣測其有還原 AnonSat 的功能。不過這部分其實連筆者都沒有真的讓自己的模型承受攻擊，其對安全性的評估僅依靠一些模型的特徵數值推測其匿名效果。

拾、課程心得

B113040002 林之謙

我在這次專題活動中學到很多，若不是有期末專題，我恐怕對衛星上網這項受人矚目的新興趨勢一知半解。同時也了解到通訊安全不只侷限於加密，算是打開了我對資安的想像。不只是知識方面，三段式的論文研究也增強了我對研究報告的閱讀理解能力，我更清楚閱讀論文時應該聚焦的重點以及心理該有的預設疑問。同時我也學到教訓，下次在選擇論文時不該過於相信助教的過濾，應該親自閱讀其中的內容評估自身能力和可達成性，再選擇自己的題目。

同時我也對於最終用 mininet 復刻感到安心同時也挺惋惜，一方面是至少還有一個容易使用且完全免費的套件可以實現我們的想法，另一方面則是對 mininet 缺乏真實物理環境的模擬感到可惜，畢竟物理環境還是實作中不可或缺的考量因素。

B113040029 曾柏諺

我在本次活動中學到很多，因為之前對網路安全比較沒興趣，所以很多新知識也是第一次接觸到。這次的專題是第一次很認真的去讀一篇論文，之前為了追求效率都是直接去找我需要的部分。經過這一次的體驗，我對資訊安全領域也是抱有了一點興趣。但看了一下我們這次讀的這篇論文的實作部分，光設備費就要15000，starlink還有月費...我來玩這個領域真的不會破產嗎?總之透過這個活動我倒是學了不少。

另外，我一定要在這邊感謝我的隊友。我這個學期因為修的課程很多，加上是單人專題，導致時間上的壓力很大。而我隊友每次報告都幫我把比較複雜或困難的部分處理了。尤其是實作幾乎都是他獨力完成的。

拾壹、組員貢獻

B113040002 林之謙
書面:
第 零、壹、貳、伍、捌、玖 節
回復 57/61 的同學問題
報告:
前1、2次的前半段 (口頭+簡報)
第三次的 實作部分
實作:
Sate.py
Readme
錄影

B113040029 曾柏諺
書面:
第 參、陸、柒 節
回復 4/61 的同學問題
報告:
前1、2次的前後段 (口頭+簡報)
第三次的 論文結果分析部分
實作:
少量意見提供，測試

拾貳、問答

B102010038 董宥弦
三角定位和時間定位的優缺點是什麼?

A: TOA 實作上簡單，不須同步時間，但精度不及 TOA / TDOA，後者實作複雜。

B113040046孫譽宸
請問衛星定位法中哪一個的精度是最高的，他有什麼硬體或軟體的要求嗎 為什麼大家不全都用精度最高的方法
A: TOA擁有最高精度，但需要使裝置間能同步時間。

B113040048 曾柏蒼
若駭客能在匿名情況下入侵中繼節點，是否會因此放大安全風險？
B103040008 許廷豪
若有中繼節點被突破的可能性，且敵方在匿名狀態下駭入了中繼節點，是否會造成更大的危險?
A: 有可能，但本次實驗模型並不考量 Gateway 被駭的情況
b113040018張軒與
海底電纜與衛星通訊在傳輸品質上是否存在明顯差異？若通訊過程中發生路徑切換，是否有可能出現數據延遲或遺失的情況？
A: 目前衛星上網的延遲和帶寬方面都比海底電纜還要弱，因此傳輸品質還是電纜更勝一籌，在大數據傳輸上更禿顯衛星上網的弱勢。當然是可能有延遲或遺失，但這部分應該是由傳輸層協議處理，而衛星上網應該是應用層的技術，因此並非在研究範圍內。

B113040052 陳育霖
未來是否可能結合類似「假訊號產生器」來擾亂三角定位？
A: 有可能，但雷達電波並非點到點，友軍可能因此受到波及，而且修正波型仍需仰賴前導序列，因此傷敵一千自損八百的可能性高。

B113040010楊諺涵
簡報有圖示輔佐說明，講解很清楚，請問此篇論文勿目標為何？
A: 解決衛星上網伴隨的使用者定位曝光問題

B103040028 林守凡
在軍事應用中，是否存在專用的匿名通訊協定能結合衛星傳輸？
B113040011 沈柔薰
為什麼即使採用 TLS 或 Tor，仍無法避免被三角定位？
B113040015。張詠捷
既然我們都有 TLS、VPN、Tor 之類的方案可以加密流量，那為什麼作者覺得這些都解決不了衛星 Internet 用戶被三角定位的問題，反而要在 IP 網路層跑一圈自動化的 Mesh＋Gateway 跳轉？
A: 不行，三角定位依賴的物理特性是不須知道通訊內容的。作者並沒有說要用IP層，只是文中有介紹並解釋傳統問路的不足。

B113040058 向子聰
對衛星的攻擊只有定位這種嗎?還是有可能會有其他的攻擊呢?
A: 你可以學后羿把馬斯克的衛星射下來

B113040045 許育菖

平面的三角定位至少要三個基準點沒錯，但衛星的三角定位應該至少要四顆衛星才能實現喔，因為有(x, y, z)以及相對論產生的時間差t四個變數需要計算。
A: 你是對的。抱歉，我們查到的論文沒有解釋這麼多

B105040024 林以晴
既然電磁波的物理特性難以隱藏，那還有什麼方式可以提高衛星通訊的地理匿名性？
B113040031 李子崴
提到定位資訊容易被利用，有哪些防禦機制可以有效減少這類風險？
A: 用 AnonSat

B113040049 陳舜邦
你們提到透過多個 gateway 分流可以隱藏使用者位置，那如果有一個中繼節點被攻擊者入侵，會不會就有可能被推回原始來源？
A: 會的，所以其 routing 內容採取隨機多跳且具有 timeout 的設計可以更換 route 和 uplink gateway。

B113040008 吳政翰
如何去測試方法的成本要求
A: 那是製造商的工作和研究者無關。

B133245006李育陞
衛星網路是否會因密集度過高導致設備相互影響
A: 會的，頻道重疊導致訊號互相干擾，其他高能光波也有可能干擾訊號，星鏈間也有可能彼此桿數。

B133040054 鄭敦翰
低轨道卫星（如Starlink）的通讯为何易受网关-卫星链路监听？
A: 三角定位

B113040041蔡昌燁
在有限頻寬下，如何兼顧隱私保護與資料傳輸效率？
B112040003 張景旭 to 第16組
行動通訊其實也會被定位，那衛星定位比起地面系統有什麼特別難防的地方？
A: 位置曝光的主要威脅和頻寬無關，是雷達電波物理特性無法隱藏。

B133245012 黃朝暉
使用衛星連接網路的成本會比電纜還要低嗎？
A: 問成大跟中央。

B113040035 羅永倫
第16組 舉例清晰 但在簡報上好像沒有很詳細得說明攻擊方式
A: 罰你重聽。

B113040036 張鳳愷
第16組 衛星定位是否也有可能被攻擊呢

A: 可以用三角定位鎖定位置。

B103040004 陳俊宇 To 第十六組
preamble header 跟一般封包的 header 有什麼區別嗎？
A: preamble header 是實體層專用，功能包括: 編碼方式、資料長度、傳輸速率等，同時還能同步裝置時間。但不是點對點，不像一般 header 有紀錄目標或發信源地址等功能。

B133040055 劉立玉
第十六組:TOA和TDOA差在哪裡？哪一個對於定位更實用？
A: TOA 需要紀錄絕對時間，反之 TDOA 只要記錄時間差，因此 TDOA 更加容易使用，’限制也比較少。

蕭維亨 B103040063
三角定位法對於三顆衛星之間的距離有規定嗎？(組別16)
A: 並沒有要求特定距離，但是對幾何分部有要求(入射角 etc)

B113040028呂蔚 第16組問題:
AOA 為什麼至少需要兩個以上的接收器才能定位？
A: 為何你求點座標需要兩條有焦點的直線公式?

B113040022周磊 to16組
TLC喝PTConnect如果同步運作的話會不會有不兼容的風險
A:我為了你重看了我們的報告三次，還是沒找到哪裡有提到這些東西，也沒印象論文有這些。你是不是填錯組別了?看時間應該是要問14組。

B113040049 陳舜邦 你們設計了 Gateway timeout 機制來輪換路徑，那在高延遲環境下，這樣會不會導致頻繁切換反而降低通訊穩定性？
B113040017 林玟妗 第十六組:Gateway timeout 的最佳時間要怎麼選擇？
A: 會的，因此作者才沒給定值，需要配合實際情況決定

B113040059 黃聖傑 感覺有後面講的有些趕了，好奇你們之後的實驗模擬做得出來嗎。畢竟模擬startlink感覺就好難。
b113040018 張軒與 這在實作實驗上成本上會不會過高?
B113040001李玠廷 組別13 To16:實作上會不會造成太大的困難
B103040031楊宗諺 第十六組:starlink的成本不低，對於實驗會考慮實際購買進行測試嗎？
B113040008 吳政翰 請問預計如何設計實作方法
B133245006李育陞第十六組:這在實作實驗上成本上會不會過高?
A: 我們會先調查有無方法能用軟體呈現此模型，如不行再跟助教商量。

B113040058 向子聰 第十六組:請問各需求的優先級是怎樣的
B113040035 羅永倫 to 第16組 :簡報中提到的四個需求非常重要，請問這些需求的優先級是什麼？在實際部署中，如何權衡這些需求？
A: 這些要求彼此間並沒有衝突，因此沒有優先順序的問題。

B133040055 劉立玉 組別6 第十六組：怎麼確保所有Gateway都能正確且即時地執行timeout和重新選擇路徑的機制？
A: 這部分因該用的 SDN 決定，但是作者在文中並未提及這一部分，所以 gateway fail的部分並不予討論，而 timeout 本身是由 client自己維持 timer，所以不會因其他 router 而無法正確執行。

B103040008 許廷豪 第十六組 問題：這種依賴衛星的技術若遇到國安問題無法使用該如何處理?
A: 麻煩請示軍事研究者、國防部發言人及現任三軍統帥。

B105040024 林以晴 第十六組：你們的系統設計中用了很多保護機制，那在實際使用上有遇到什麼問題嗎？
A: 會在第三次報告時提及。

B103040033 吳尚恩 第十六組 在部署過程中，有無考慮資料蒐集階段對用戶隱私的可能侵犯？
A: 這和電信服務相同道理，如果沒有註冊就無法使用，因此沒有所謂「侵犯」，一旦都是你情我願。

B113040045 許育菖 想問作者有說要傳遞原始資訊要透過gateway傳遞多遠才比較有效嗎？而且如果是透過其他的gateway來傳遞資訊的話，那變成其他gateway的地理資訊會洩漏給衛星，進攻方只要每發現一個gateway位置就進行攻擊就好了。
A: 這篇文章擔心的是使用者的位置洩漏使得有心人士可以對其進行暗殺，因此亂槍打鳥是無法達成目的，即使成功攻下一個 gateway 也不保證能攔截到特定訊息來找出客戶端的位置。

B103040004 陳俊宇 To 第十六組 如果用戶設備同時有多種上網方式（如蜂窩網路、地面光纖），整體的隱私保護效果是否會下降？
A: 在 host 到 ISP的部分仍和以往的形式相同，可能會，但此實驗模型已先預定除衛星上網外的形式皆已失效。

B113040031李子崴 第十六組：當 LoRa hops 增加時，RTT 與封包遺失率持續上升，這樣的延遲是否會限制實際應用？
A:會直接影響到直播，網路電話這種有即時性需求的東西。另外可能會因為延遲過高/重傳次數過多而不被網站信任

蕭維亨 B103040063 組別6 第十六組：什麼是Lora格式？和機器學習裡的Lora是同一個東西嗎？

B113040041 蔡昌燁 加入方向偏好 θ 與權重後，攻擊者的分布推估會有盲點嗎？
A: 別說盲點，攻擊者已無法用分布推測使用者位置。

B103040028 林守凡，對第十六組：Distance to Origin 提到太遠雖安全但效率差，是否也考慮以 latency 作為衡量的折衷調整參數？

B113040052 陳育霖 gateway timeout 是為了避免整條路徑被追蹤，但這樣頻繁換 gateway 會不會導致連線品質下降？
A: 會，作者已說需要因應實際情況決定數值來避免某一缺點過度明顯。

B113040028呂蔚 Output Selection Bias這種方法是否適合應用在高密度城市環境？
A: 只要有足夠 gateway就好，在哪都一樣。

B113040015。張詠捷 第十六組：既然攻擊者靠的是衛星之間的時差來推算發射位置，那為什麼 AnonSat 不直接在用戶端加一點延遲，而是設計成把流量轉發到遠端 gateway ？
A: 首先，筆者並未提及是用哪一種三角定位法攻擊。再來，這邊的時間差是同一訊號被不同衛星偵測到的時間差，即使在本地網路中加入 latency 也無法對訊號的上鏈造成影響。

B105040024 林以晴 第十六組：你們在實作 AnonSat 模型時，有沒有遇到哪部分在模擬環境中特別不好處理？
A: 意外的沒有，也可能是我們的自製模型過於簡易僅專注在實現文中提到的機制。而忽略網路系統中更深刻的問題。

B103040004 陳俊宇 第16組 如果無法模擬這些關鍵因素，那麼實驗結果如何反映真實世界中的匿名化效果和對抗攻擊的能力？
A: 我們的實作僅聚焦於在作者沒有分享任何資源的情況下，盡可能還原其在先前實作的模型，因此並沒有考量實際的安全能力。作者自己也是拿數據推測其能力而非真實進行實戰。

B133245006李育陞
第16組 實質匿名集跟理論匿名集的差別在哪裡?
A:理論匿名集只考慮了有可能是來源的數量，就算實際上在攻擊者方能得知某個節點為實際來源的可能性<0.1%，在理論匿名集中仍然會被計錄為1。但實質匿名集則會整合所有線索來決定猜測來源的真實難度，進而反映出比較真實的匿名強度。

B113040058 向子聰 第十六組: 請問在不同地區或地形會有影響嗎
B113040015。張詠捷 第十六組：衛星通訊在地理分布或使用者位置差異上有效能影響
A: 會的，本地網路間節點的距離也會造成傳輸影響，節點間若用無線電波傳訊也有可能會有繞射、散射、波形崩壞等問題。

B113040017 林玟妗 第十六組：為什麼作者也沒有實作攻擊的部分
A: 推測是是因為真實的衛星使用權較難取得，且團隊實作的概念模型規模也不大，特地準備衛星有點大材小用。且此文在一開始就只針對三角定位法，所以也可以單純從數據推估攻擊性吧。

B113040041 蔡昌燁 第十六組：是否考慮 adaptive timeout？
A: 我們沒想到，但這是個不錯的考量，可惜每次 routing 的路徑和跳數都是隨機，如果用 adaptive timeout 或許不合呼原本的用意，反而擴大風險。像是前一次 RTT 比較常所以拉長 timeout，結果這次 route很短，攻擊者有很長的時間可以逆向追蹤。

蕭維亨 B103040063 第16組:用python的miniet會模擬使用衛星通訊的物理特性如不同地區的user？
A: 我應該說過 mininet 無法模擬物理、地理特性了。

B113040028呂蔚 16 : 和 NetEm 結合時是否有遇到相容性問題或設定困難
A: 無，頂多只有 apt 版本不相容，下載時有修改。

B112040003 張景旭 第十六組 你們在 Mininet 架構下模擬多跳傳輸，請問這樣的模擬對實際衛星網路場景的代表性夠嗎？
A: 缺點已提出，明顯是不夠，請專心聽課。

第16組: 在實際部署中，攻擊者是否可能故意破壞某些關鍵節點來降低整體匿名性？
A: 可以，但這對此專案來說是無效命題，因為在作者理想的 AnonSat 中每個 gateway 都有幫忙上鏈及充當 router 的功能，引此並沒有關鍵節點。