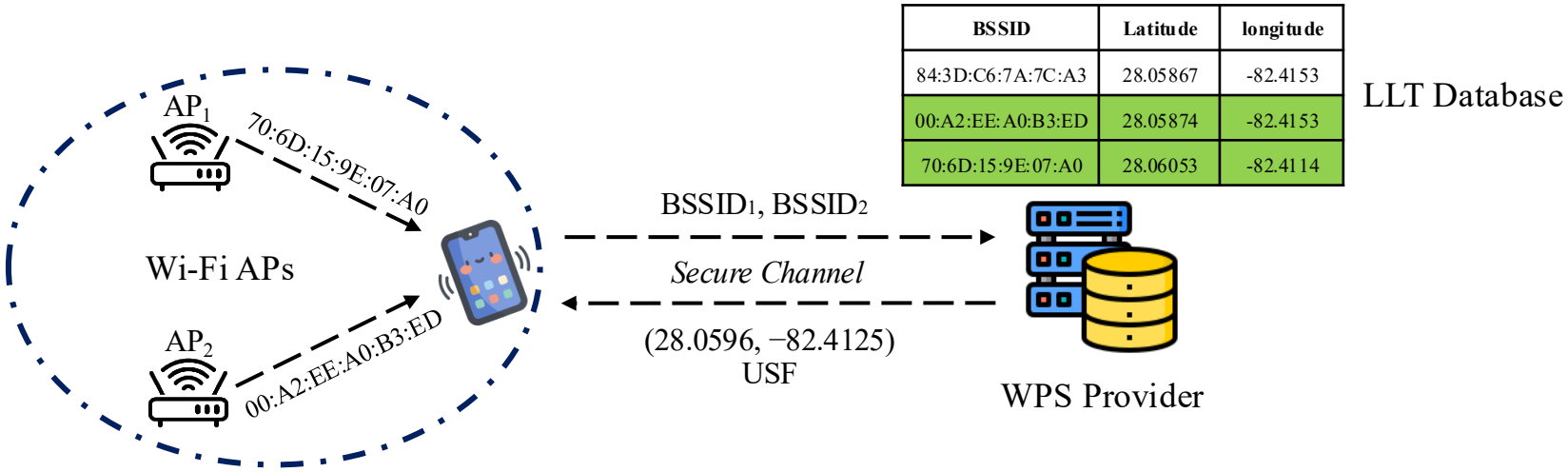
# WILD Attack: Stealthy Undermining of Wi-Fi-Based Geolocation Through Remote Crowdsourced Data Injection

Changjia Zhu, Xiao Han, Parush Gera, Zhuo Lu, Tempestt Neal, Yao Liu

University of South Florida



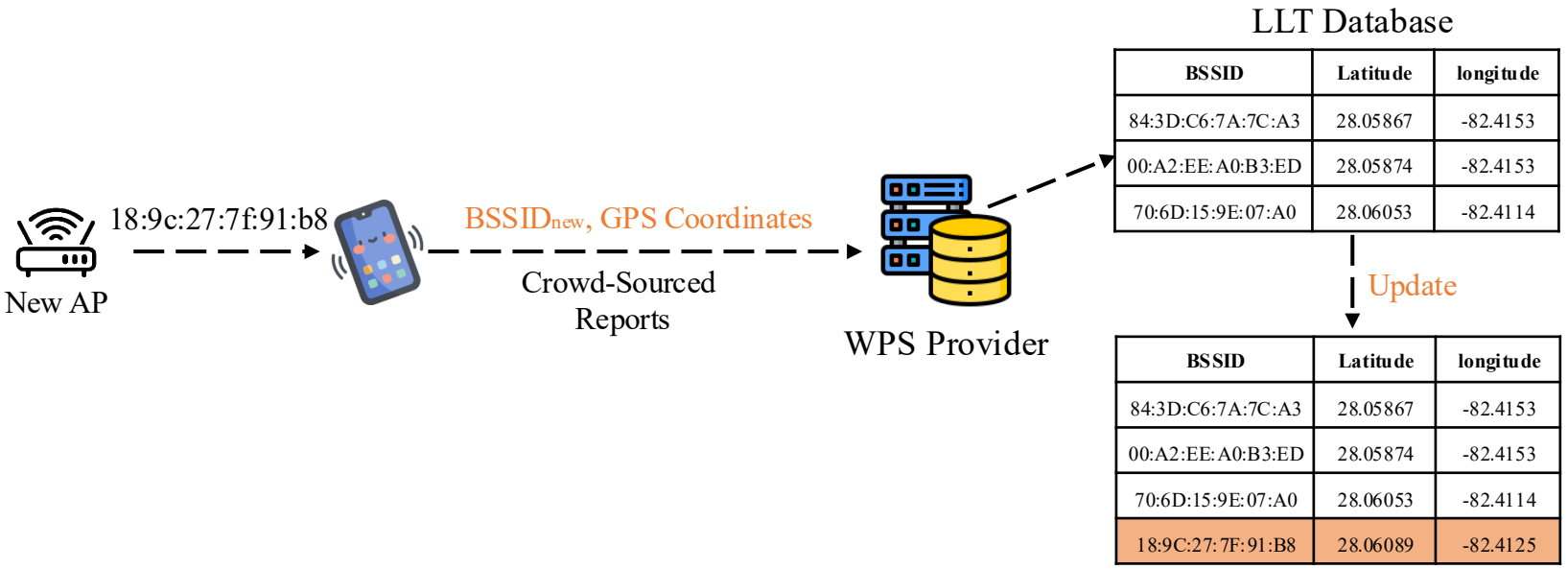
# Wi-Fi Positioning System




Wi-Fi Positioning Systems (WPS) complements GPS, especially indoors or in dense urban areas.

Mobile devices query the WPS provider using the BSSIDs of nearby access points (APs). The provider looks them up in the Location Lookup Table (LLT) and returns an estimated location.

# Crowd-Sourced Reporting



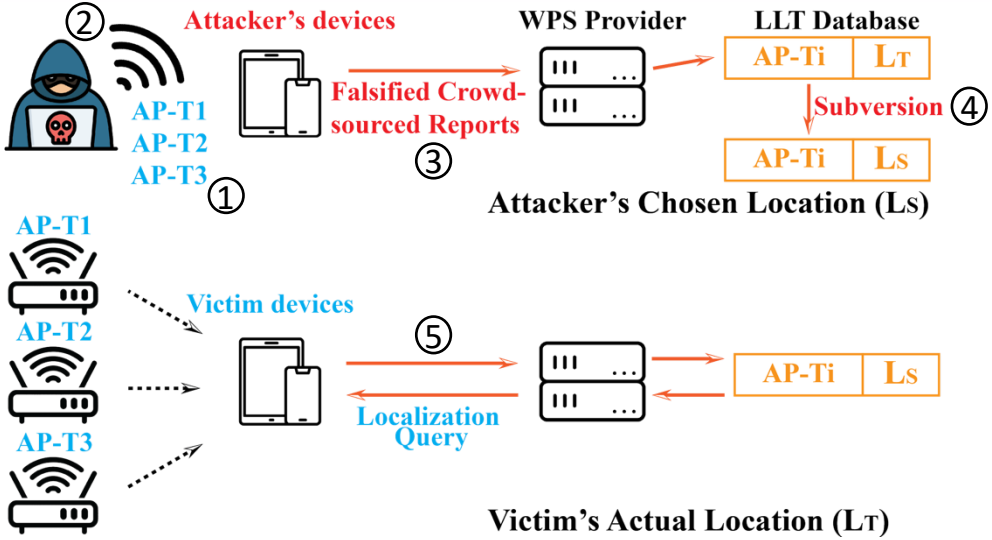

| BSSID | Latitude | longitude |
|---|---|---|
| 84:3D:C6:7A:7C:A3 | 28.05867 | -82.4153 |
| 00:A2:EE:A0:B3:ED | 28.05874 | -82.4153 |
| 70:6D:15:9E:07:A0 | 28.06053 | -82.4114 |

| BSSID | Latitude | longitude |
|---|---|---|
| 84:3D:C6:7A:7C:A3 | 28.05867 | -82.4153 |
| 00:A2:EE:A0:B3:ED | 28.05874 | -82.4153 |
| 70:6D:15:9E:07:A0 | 28.06053 | -82.4114 |
| 18:9C:27:7F:91:B8 | 28.06089 | -82.4125 |

During WPS localization, mobile devices send crowd-sourced reports containing BSSID and GPS coordinates.

WPS providers rely on the crowd-sourced reports to maintain and update the LLT for newly deployed or relocated APs.

# Attack Methodology

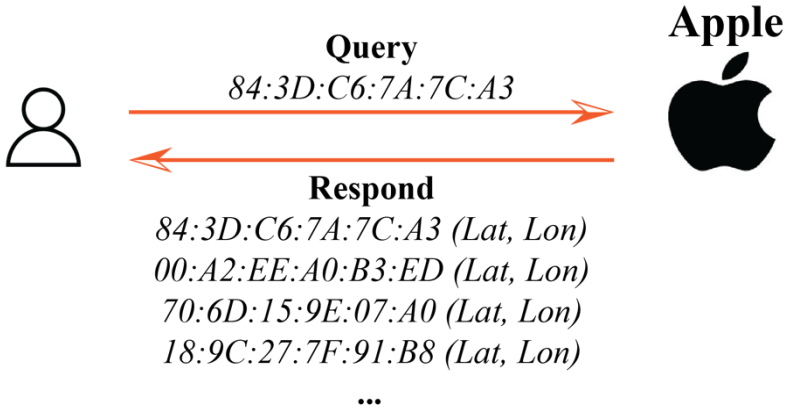



By submitting falsified crowd-sourced reports, an attacker can undermine the integrity of WPS.

**Attack workflow:**

① Collect the target BSSIDs near the victim;
② Broadcast forged Wi-Fi signals using these BSSIDs;
③ Attacker-controlled or nearby unwitting devices receive the forged signals and submit crowd-sourced reports;
④ LLT entries subversion;
⑤ Victims receive falsified WPS localization.

# Target BSSIDs Collection





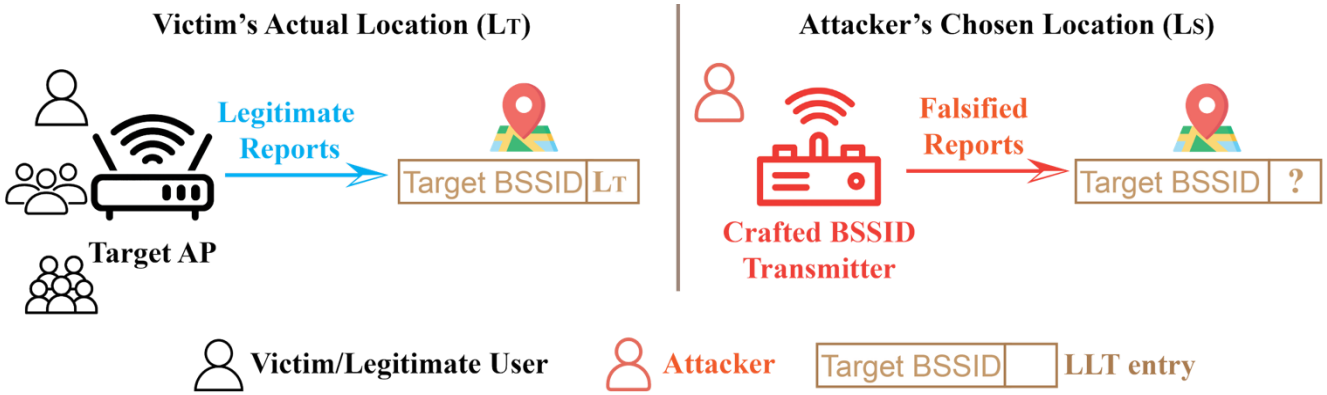


When queried, Apple WPS returns neighboring BSSIDs in addition to the queried one.

The neighboring BSSIDs can extend up to 300 meters from the queried BSSID.

**Hop-by-Hop Expansion**: Iteratively query newly discovered BSSIDs that are progressively closer to the target location.

# Conflict between Legitimate and Falsified Reports

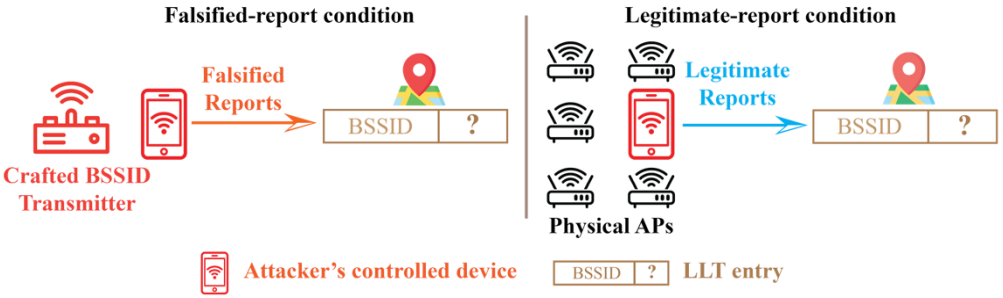



Target APs continue to operate near the victim, so legitimate devices still submit legitimate reports.

WPS providers therefore receive conflicting reports regarding the same BSSIDs from different locations.

Whether the LLT can be subverted depends on how the provider handles such conflicts, i.e., **conflict-resolution policy**.

# Hypotheses on Conflict-Resolution Policy







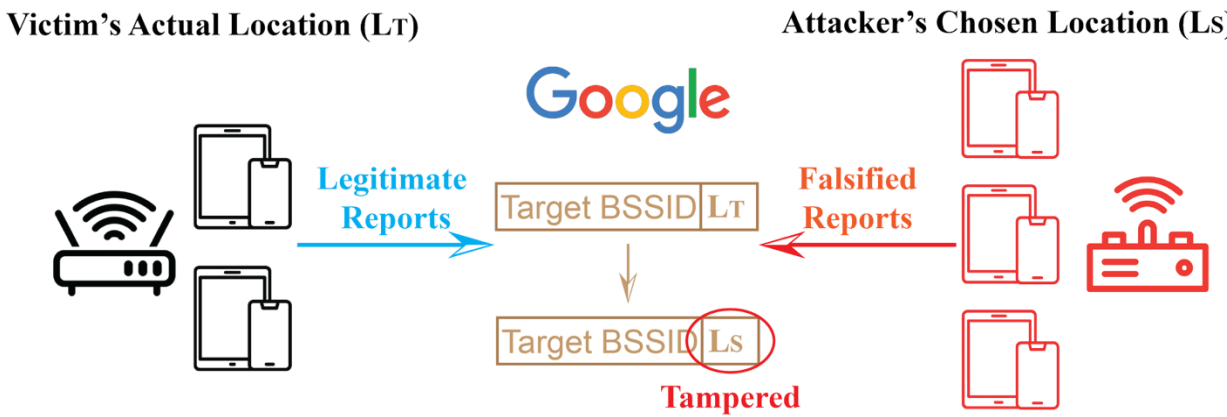
Determine whether reports from distinct locations ($L_A$ and $L_B$) are treated as collaborative or competing.

If they compete, which policy does the provider use to resolve the conflict?

We hypothesize four policies: (1) majority-wins; (2) last-report-wins; (3) each-report-counts; and (4) zero-trust.

Reverse-engineer each provider's policy by manipulating the spatial and temporal characteristics of conflicting reports and probing the LLT entries.

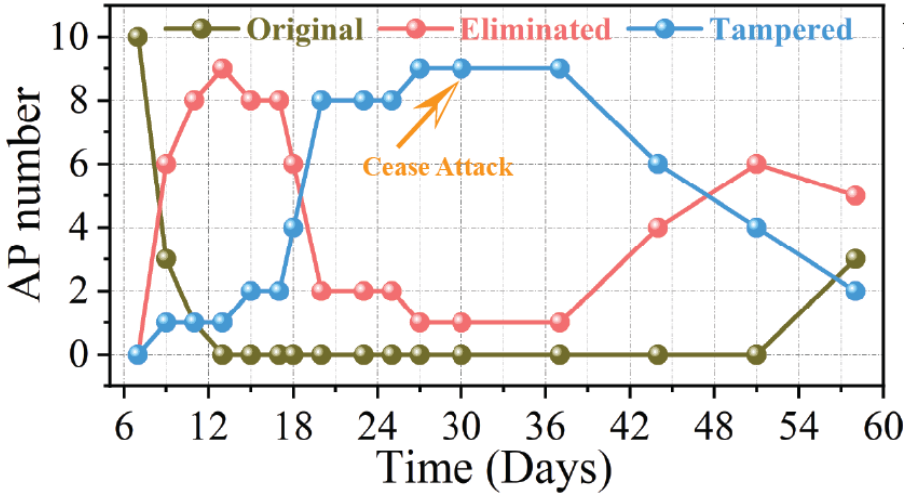
# Majority-Wins Policy




Google WPS adopts a **majority-wins policy**.

Once the volume of falsified reports exceeds that of legitimate ones, the corresponding LLT entries are tampered with.

# LLT Entry Tampering



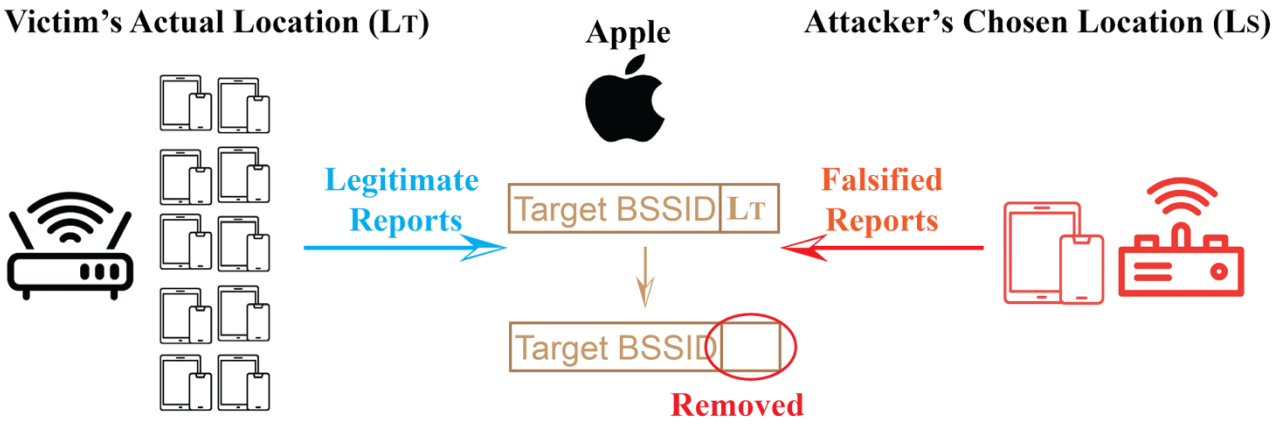

Google WPS subversion follows a two-phase **LLT Tampering** pattern,

**Phase 1**: original LLT entries are eliminated;

**Phase 2**: tampered LLT entries are created.

The attack effect persists for weeks, even after the falsified reports cease.

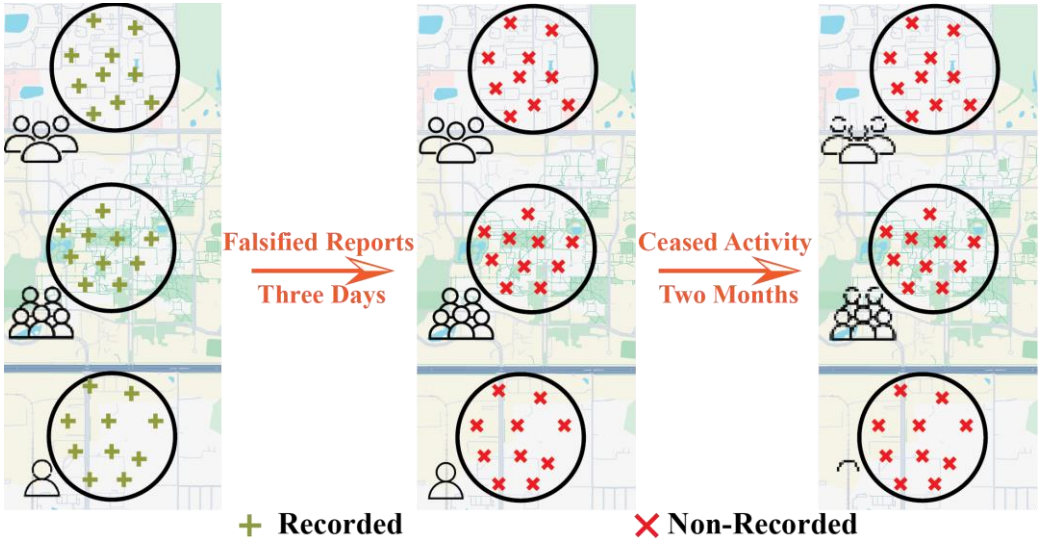
# Zero-Trust Policy




Apple WPS adopts a **zero-trust policy**.

Even with a few falsified reports (e.g., one-tenth of the legitimate reports), Apple WPS trusts neither source.

# LLT Entry Removal

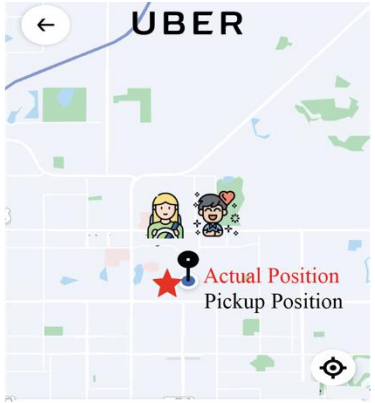



Apple WPS subversion follows a **LLT Removal** pattern

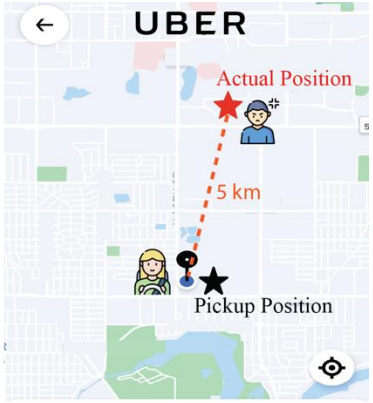
The LLT entries corresponding to the target APs are removed after three days of falsified reports.

The attack effect persists for two months after the falsified reports cease.

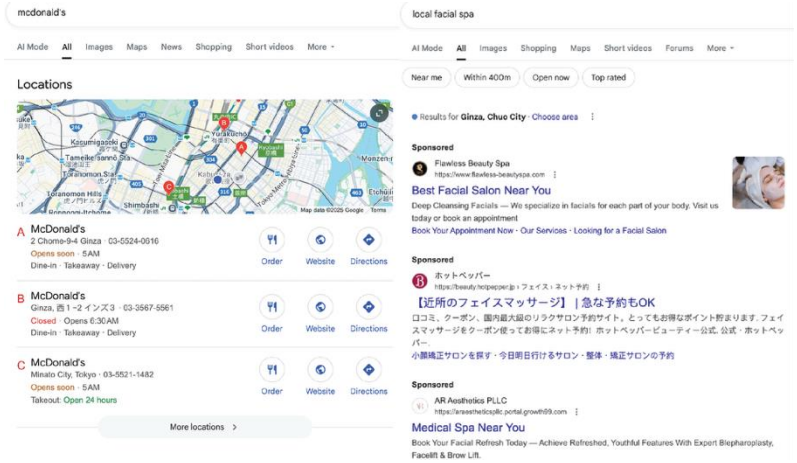
# Real World Impact




(a) Before the attack




(b) After the attack




On an Android device that relies on Google WPS, Uber automatically selected a pickup point at the tampered location.

Location-related queries, such as “McDonald’s” or “local facial spa”, return results and advertisements for the attacker’s chosen location, instead of the victim’s actual location.

The attacker can thus hijack customer traffic from the competitor.

# Thank You!

Feel free to connect through LinkedIn



Homepage: https://changjiazhu.com/
Email: changjiaz@usf.edu