УДК 004.891

О.В. КЛІЩ, О.В. ОГНЄВИЙ
Хмельницький Національний університет

МЕТОД ВІДСЛІДКОВУВАННЯ МОБІЛЬНОГО ПРИСТРОЮ ЗА ПЕРЕХОПЛЕНИМИ «ПРОБНИМИ» ПАКЕТАМИ ПІДКЛЮЧЕННЯ ДО WIFI

На сьогоднішній день майже у кожного є пристрої із вбудованим WiFi модулем, для можливості підключення до бездротових мереж. Більшість із нас за день підключається до кількох бездротових мереж: вдома, на роботі, в кафе і т.д. У даній статті ми звернемо увагу на принципи утворення WiFi з'єднання між точкою доступу (роутером) та портативним пристроєм, розглянемо відмінності підключення різних пристроїв, а також типи «пробних» пакетів. На основі проведених досліджень було вибрано найбільш прості та доступні ресурси для вирішення поставлених завдань, розглянути недоліки і переваги створюваного методу, а також перспективи його доопрацювання та застосування.

Ключові слова: WiFi, точка доступу, пакет, відслідковування.

O.V. KLISHCH, O.V. OHNIEVYI
Khmelnitsky National University

METHOD OF TRACKING MOBILE DEVICE BY INTERCEPTED "TRIAL" FRAMES OF CONNECT TO WIFI

Abstract - Aim of the article is a justification of this method of trackin, its differences and Aim of the article is a study on this method of tracking its differences and features, compared to other methods of tracking. Nowadays almost everyone has a device with built-in WiFi module for connectivity options to wireless networks. Most of us during the day connects to some wireless networks: at home, at work, in cafes, etc. In this article we turn our attention to principles of creating Wi Fi connection between the access point (router) and portable device , consider the differences between various connection devices and the types of "test" packages.

Based on conducted research was chosen the most simple and available resources to solve the assigned tasks, consider the advantages and disadvantages of created method and perspectives of its improvement and use.

Key words: Wi-Fi, access point, package, tracking.

Постановка задачі

Існує декілька основних способів визначення місцезнаходження пристрою:

- За унікальним номером IMEI. Проте здійснити це дуже важко, оскільки для цього потрібно звернутися до оператора мобільного зв'язку, і таку інформацію фізичним особам не надають.
- За допомогою технології GPS, але дану технологію підтримують далеко не всі портативні девайси і вона потребує додаткового ПЗ або налаштувань на шуканому пристрої.
- Існують також спеціальні додатки для знаходження загубленого пристрою, деякі з них обіцяють застосування кількох різних методів.

Проте жоден з них не можна повноцінно порівняти із описаним мною методом. Оскільки кінцевим результатом нашого методу буде історія підключень пристрої, а звідси й історія місцезнаходження пристрою. А найголовніше, що для цього нам не потрібно встановлювати жодного додаткового ПЗ на пристрій, і не обов'язково бути його власником.

Виклад основного матеріалу досліджень

Технологія Wi-Fi цікава в концепції тим, що одна базова станція мережі системи Wi-Fi може дати доступ десяткам абонентів відразу, причому з досить більшими швидкостями. Мінімальні вкладення і простота реалізації роблять Wi-Fi цікавою та широкозастосованою технологією.

Той факт, що у всіх сучасних портативних девайсах реалізовані функції Wi-Fi, полегшує застосування цієї технології в публічних місцях. Більшість користувачів за день підключаються до кількох точок доступу: вдома, на роботі, в кафе і т.д. Отож завданням данного методу є визначення точок доступу до якмх підключався користувач, та визначення їх місцеположення. Існують й інші методи відслідковування місцеположення девайсу, та наше завдання здобути якомога більший список мереж, до яких користувач підключався, для отримання більшого об'єму інформації про власника девайсу.

Важливо відзначити, що користувацькі пристрої можуть працювати в двох режимах пошуку мережі [2,ст.37]:

1. Режим Пасивного сканування (Passive Scanning) - досить повільний режим, тому користувацький пристрій повинен послідовно прослуховувати всі частотні канали підтримуваного діапазону в надії виявити бікони (Beacon Frames). Ці пакети розсилають роутери, щоб оголосити про свою присутність[3]. Клієнт знаходить вже відому йому мережу і з'єднується з нею. Такий режим, зазвичай, використовують ноутбуки та інші пристрої, які не є смартфонами.

2. Режим Активного сканування (Active Scanning) - активно відсилаються запити в ефір. Пристрій посилає фрейми типу Probe Request по всіх частотних каналах в підтримуваному діапазоні часто із зазначенням шуканого SSID мережі (direct probe request) або без SSID (null probe request). Активне сканування значно підвищує динаміку роботи з мережею і допомагає у вирішенні таких завдань, як, наприклад, забезпечення швидкого роумінгу і т.п., але і створює деяке додаткове навантаження на мережу.

Взагалі стандарт 802.11 визначає три типи фреймів:

1. Фрейми Управління (Management frames).

Фрейми управління 802.11 дозволяють встановлювати і підтримувати комунікації в мережі стандарту WiFi.

Всього стандарт 802.11 визначає 14 типів фреймів управління:

1. Association request,
2. Association response,
3. Reassociation request,
4. Reassociation response,
5. Probe request,
6. Probe response,
7. Beacon,
8. ATIM (Announcement traffica indication mesage),
9. Disassiciation,
10. Authentication,
11. Deauthentication,
12. Action,
13. Action No Ack,
14. Timing advertisement.

2. Фрейми Контролю (Control frames).

Фрейми контролю 802.11 допомагають у доставці фреймів даних між станціями і точками доступу. Всього стандарт 802.11 визначає 9 типів фреймів контролю:

1. PS-Poll (Power Save Poll),
2. RTS (Request to Send),
3. CTS (Clear to Send),
4. ACK (Acknolegement),
5. CF-End (Contention Free-End),
6. CF-End + CF-ACK,
7. Block ACK Request (BlockAckReq),
8. Block ACK (BlockAck),
9. Control wrapper.

3. Фрейми Даних (Data frames).

Природно основне завдання мережі стандарту WiFi це передача даних. Фрейми Даних переносять пакети вищерозташованих рівнів, таких як веб-сторінки і т.п. всередині тіла самого фрейму. Якщо переглянути фрейми 802.11 через аналізатор пакетів, то можна розглянути контент тіла фрейма і побачити які пакети даних знаходяться всередині фрейму даних при транспортуванні.

Стандарт WiFi IEEE 802.11 визначає 15 типів фреймів даних:

1. Data frame (простий фрейм даних).

Простий фрейм даних це найбільш поширений тип фреймів даних.

2. Null function (фрейм спеціальної нульової функції),
3. Data + CF-ACK (PCF only),
4. Data + CF Poll (PCF only),
5. Data + CF-ACK + CF-Poll (PCF only),
6. CF-ACK (без данных) (PCF only),
7. CF-Poll (без данных) (PCF only),
8. CF-ACK + CF-Poll (без данных) (PCF only),
9. QoS Data (HCF),
10. QoS Null (без данных) (HCF),
11. QoS Data + CF-ACK (HCF),
12. QoS Data + CF-Poll (HCF),
13. QoS Data + CF-ACK + CF-Poll (HCF),
14. QoS CF-Poll (без данных) (HCF),
15. QoS CF-ACK + CF-Poll (без данных) (HCF).

Кожен фрейм має контрольне поле, яке визначає версію протоколу 802.11, тип фрейму і різні індикатори, як наприклад: WPA включений, управління енергозбереженням активно і т.п.. Додатково до цього всі фрейми містять MAC-адреси джерела й одержувача, номер фрейму в послідовності, тіло фрейму і перевірочну послідовність фрейму для корекції помилок. Фрейми 802.11 переносять протоколи та дані більш високих рівнів моделі OSI / ISO всередині тіла фрейму. Наприклад фрейм даних може транспортувати HTML-код будь-якої веб-сторінки (з усіма необхідними заголовками TCP / IP), використовувані далі для відображення. Інші фрейми, які станції використовують для управління і контролю, несуть специфічну інформацію про бездротове з'єднання в тілі фрейму. Наприклад, тіло фрейму-бікона містить ідентифікатор мережі WLAN: SSID, тимчасові відмітки (timestamp) та іншу інформацію про точку доступу.

Beacon frame (Фрейм Бікон) - це один з найбільш важливих фреймів керування. Точка доступу WiFi періодично відправляє їх для анонсування своєї присутності та надання необхідної інформації (SSID, частотний канал, тимчасові маркери для синхронізації пристроїв за часом, підтримувані швидкості, можливості забезпечення QoS і т.п.) всіх пристроїв в зоні її покриття. Радіокарти користувацьких пристроїв періодично сканують всі канали 802.11 і слухають бікони, як основу для вибору кращої точки доступу для асоціації. Користувацькі пристрої зазвичай не розсилають бікони, за винятком ситуації, коли виконується процедура участі в IBSS (Independent Basic Service Set) або, по іншому, в одноранговому з'єднанні типу Ad-hoc.

Probe request frame (Фрейм-запит Проба) - мобільні пристрої з WiFi відправляють фрейми-запити проби, щоб отримати інформацію від іншого пристрою. Наприклад, радіокарта мобільного пристрою відправляє Проби-запити, щоб визначити які точки доступу знаходяться в зоні покриття.

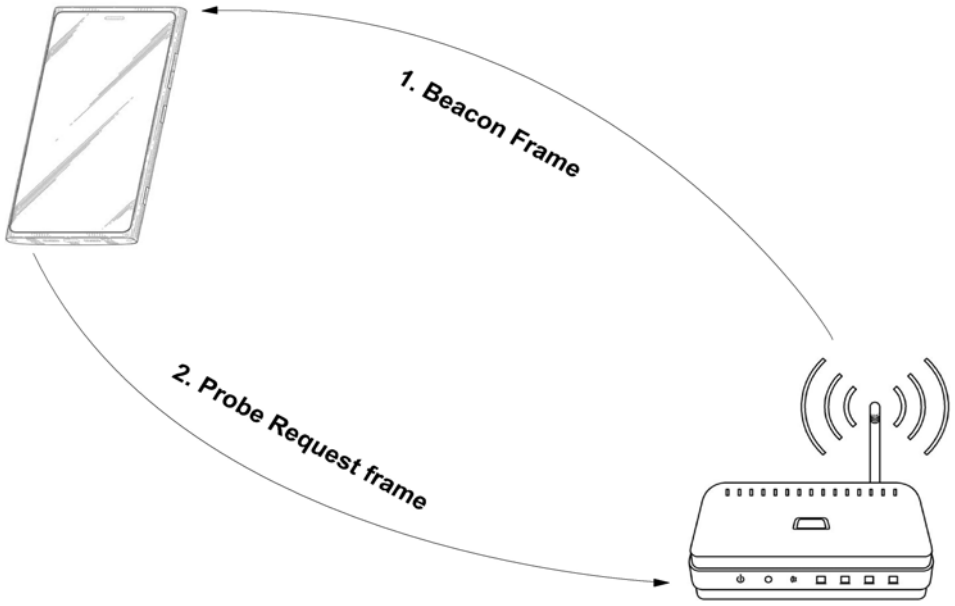

Рис. 1. Схема обміну пакетами пристрою і точки доступу

Нас цікавить Probe request frame, оскільки прочитавши саме його ми отримаємо необхідну нам інформацію, а саме - ім'я мережі та mac-адресу пристрою. Важливо, що Probe Rerquest frame містить не лише ім'я мережі до якою намагається підключитись в даний момент, а й список мереж до яких він підключався раніше. Саме на основі цього списку ми і зможемо дослідити історію підключень пристою. Ім'я мережі, в процесі дослідження, розкаже нам про розташування точки доступу. Отже ми зможемо перенести дані на карту, і отримати історію місце розташування пристрою з точністю до будівлі. А mac-адреса [4, с.30] пристрою дозволить нам дізнатись модель пристрою, що допоможе віднайти його власника в натовпі.

Висновки

Зроблені висновки про доцільність використання даного методу відслідковування мобільного пристрою. Проведений аналіз дозволив зробити висновки про доцільність використання цього методу для отримання додаткової інформації про переміщення пристрою і його власника.

Запропонований підхід дозволить швидко отримати важливу інформацію без контакту з пристроєм і додаткових дозволів.

Література

1. Wi-Fi. (Вікіпедія — вільна енциклопедія) [Електронний ресурс]. – Режим доступу до статті: https://uk.wikipedia.org/wiki/За[ист_у_мережах_Wi-Fi.

2. Джон Росс. Wi-Fi. Беспроводная сеть / Джон Росс ; пер. с анг. В. А. Ветлужских. – Москва: НТ Пресс, 2007. – 320 с.

3. Захист у мережах Wi-Fi. (Вікіпедія — вільна енциклопедія) [Електронний ресурс]. – Режим доступу до статті: https://uk.wikipedia.org/wiki/Захист_у_мережах_Wi-Fi.

4. Щербаков А. К. Wi-Fi: Все, что Вы хотели знать, но боялись спросить / Щербаков А. К.; - Москва: ЛА «Бук-Пресс», 2005. - 352 с.

Рецензія/Peer review : 27.11.2015 р. Надрукована/Printed :6.12.2015 р.
Рецензент: д.т.н., проф., Мясіщєв О.А.