Mobil eszközök követése a 802.11-es szabványban meghatározott menedzsment keretek segítségével

Mobile device fingerprinting using management frames defined in the 802.11 standard

HAJDÚ Hunor

Accenture, Marosvásárhely, Aurel Filimon utca 19A

Abstract
My paper investigates the tracking and determination of the location of mobile devices using the management frames of the 802.11 standard. Based on the data extracted from Probe, Association, and Authentication Request frames, I determine the positions of the devices and then represent them on a map. For this purpose, I developed a program written in Python. The program can analyze network traffic and draw a map based on it, as well as manage network interfaces. Additionally, to make the receivers compact and easy to deploy, I used Raspberry PI computers. I tested the program in various environments such as at the University of Medicine, Pharmacy, Science and Technology of Târgu Mureș, in an office building, and in a private home. Based on the results of the experiments, I concluded that the placement of the receivers significantly influences the amount of collected data and that ensuring the synchronization of the clocks of the receivers is important.

Kivonat
A munkám a 802.11 szabvány menedzsment kereteinek használatával követi és határozza meg a mobil eszközök helyzetét. A Probe, Association és Authentication Request keretekből kinyert adatok alapján meghatározom az eszközök pozícióját, majd térképen ábrázolom őket. Ehhez egy Python nyelven írt saját fejlesztésű programot használtam. A program képes a hálózati forgalmat elemezni és térképet készíteni annak alapján, valamint kezelni a hálózati interfészeket. Továbbá, hogy a vevők könnyen telepíthetők és kompaktak legyenek, a Raspberry PI-t használtam. A programot különböző környezetekben teszteltem, például az Marosvásárhelyi "George Emil Palade" Orvosi, Gyógyszerészeti, Tudomány és Technológiai Egytem-en, egy irodaházban és egy magánházban. Az kísérletek eredményeire alapozva arra a következtetésre jutottam, hogy a vevők elhelyezése jelentősen befolyásolja az összegyűjtött adatok mennyiségét, és fontos gondoskodni a vevők óráinak szinkronizálásáról.

1. BEVEZETŐ

A mobil eszközök elterjedése miatt jelentősen megnőtt az igény az azonosításukra és hitelesítésükre. Az egyik módszer, mely egy megbízható módon képes ezt végbe vinni: a mobileszköz-ujjlenyomat-vétel, amelynek célja az eszközök egyedi azonosítása jellemzőik és viselkedésük alapján. A dolgozatom a mobileszközök azonosításának egyik megközelítésére összpontosít menedzsment keretek segítségével, amelyek vezeték nélküli eszközök által vannak továbbítva egy adott hálózaton belüli kommunikáció érdekében.

A mobil eszközök azonosításának fontosságát nem szabad alábecsülni, mert alapja többek közt a biztonságnak, az adatvédelemnek. A már kidolgozott azonosítási technikák legtöbbször hardver vagy szoftver információkra alapulnak, amik könnyen módosíthatóak. A módszer melyet kidolgoztam, a menedzsment keretekben lévő információkat használja fel annak érdekében, hogy meghatározza az eszközök helyzetét.

Dolgozatom a következőképpen épül fel: Az 1. fejezetben bemutatom a mobileszközök azonosításának már meglévő módszereit, ezeknek alkalmazásait és kihívásait. A 2. fejezet részletesen áttekinti a felhasznált hardware-t, illetve szoftver technológiákat. A 3. fejezet bemutatja a felépített alkalmazás tervezésének

fázisait. A 4. fejezet ismerteti az implementált programot, és annak felhasználási módjait. Az 5. fejezet bemutatja kísérleteim eredményeit.

Dolgozatom célja, hogy hozzájáruljon a vezeték nélküli hálózatokon lévő eszközök azonosításához és feltérképezéséhez.

A következőekben bemutatók néhány tanulmányt mely már alkalmazza az eszközök ujjlenyomatozását, és röviden tárgyalom az általuk alkalmazott módszereket.

A következő tanulmány egy passzív ujjlenyomatozási módszert javasol, annak érdekében, hogy megőrzzük az eszközök adatainak védelmét. A ``Analyzing Passive Wi-Fi Fingerprinting for Privacy-Preserving Indoor-Positioning" [1], amely úgy szeretné ezt elérni, hogy ahelyett hogy a Probe-at gyűjtené be, inkább a Beacon keretekre fókuszál. Ezeket folyamatosan begyűjti miközben a csatornákat váltogatja. Ezáltal megkapja minden hozzáférési ponttól, és létrehoz egy ujjlenyomat vektort melyet megtölt a begyűjtött jelerősség értékekkel ezekből a Beacon keretekből.

A ``Overview of WiFi fingerprinting-based indoor positioning" [2] több módszert is felsorakoztat ami alapján meg lehet határozni egy eszköz helyzetét egy adott épületen belül, amelyek között megjelenik a WiFi is, amit az én munkám is használ. Ehhez ez a tanulmány is a begyűjtött jelerősség értékeire alapozó ujjlenyomatozást alkalmazza, valamint felsorakoztatja ennek az előnyeit és hátrányait. Nevezetesen az előnyök a következőek:

- Nincs szükség speciális hardverre
- Alacsony költségű
- Széleskörűen lehet alkalmazni

A hátrányai pedig:

- Nehéz az
- Ronthatja a WiFi jelet

A ``Device Fingerprinting in Wireless Networks: Challenges and Opportunities" [3] több módszert is tárgyal, egyaránt passzív módszereket valamint aktívakat is. Az aktív módszer amit bemutat már alkalmazva volt egy másik tanulmányban, nevezetesen a ``Active behavioral fingerprinting of wireless devices" [4] című cikkben, melyben kiküldtek nem szabványos kereteket, majd a válaszok alapján ujjlenyomatozták az eszközöket. Ezen kívül tárgyalnak olyan passzív módszereket is, amelyekkel ujjlenyomatozni tudják az eszközöket az által, hogy kivonnak a keretekből információkat amik a következők lehetnek:

- Adatátviteli sebesség váltás
- Aktív szkennelés
- Az időszinkronizációs funkció (TSF) bélyegekből származó órajel-eltolódás
- Különböző radiometriai jellemzők
- Véletlenszerű visszalépési idők
- Időtartam mező értékek az 802.11 adat- és vezérlőkeretekben
- Érkezési idők közötti intervallumok (ITA-k)

2. FELHASZNÁLT TECHNOLÓGIÁK

A mai modern világában a technológia gyors fejlődése miatt a projektem sikeréhez elengedhetetlen volt a helyes döntések meghozatala ezen a területen. A technológiák bemutatása nemcsak a projekt kontextusának megértéséhez fontos, hanem azt is mutatja, hogyan befolyásolják a fejlesztés során hozott döntések a végső eredményt.

Hardver szempontjából több Raspberry Pi-t használtam vevőként, aminek nagy előnye, hogy könnyen elhelyezhetők és sokszorosíthatók, csupán egy 16 gigabájtos SD kártyára van szükség. A vevőkön fut egy Kali Linux rendszer, melyben az általam írt alkalmazás szolgáltatásként fut, minden indításkor, emiatt elég a PI-t csupán áram alá helyezni ahhoz, hogy az adatok begyűjtése és mentése megkezdődjen. Főként háromféle keretre összpontosítottam: Probe Request, Authentication Request és Association Request, amelyek kulcsfontosságúak ahhoz, hogy egy eszköz kapcsolatot tudjon teremteni egy hozzáférési ponttal. Az elfogott kereteket PCAP fájlokban tároltam, melyek alkalmasak a hálózati adatok rögzítésére.

A Probe Request típusú kereteket eszközök küldik a hozzáférési pontok felé, hogy megtudják, milyen hálózatok érhetők el a közelben. A hozzáférési pontok ezekre a keretekre Probe Response típusú keretekkel válaszolnak, amelyek tartalmazzák a hozzáférési pont hálózatával kapcsolatos információkat.

Az Authentication Request típusú kereteket az eszközök a hozzáférési ponthoz küldik az azonosításhoz. Ezt követően a hozzáférési pont Authentication Response típusú keretet küld vissza, amely megerősíti az eszköz azonosítását.

Az Association Request típusú kereteket az eszközök a hozzáférési ponthoz küldik a hálózathoz való csatlakozáshoz. Ezt követően a hozzáférési pont Association Response típusú keretet küld vissza, amely megerősíti, hogy az eszköz most már hozzáféréssel rendelkezik a hálózathoz.

A PCAP (Packet Capture) egy olyan fájlformátum, amelyet a hálózati adatcsomagok rögzítésére használnak, amelyek későbbi analizálhatók. A PCAP fájlokban tárolt információk sokféle hálózati eseményt tükrözhetnek, beleértve az adatcsomagok átvitelét, a hozzáférési pontok és készülékek közötti kommunikációt, valamint esetleges hálózati hibákat is.

3. TERVEZÉS

A programom tervezése során fontosnak tartottam a munka felosztását több részre annak érdekében, hogy megkönnyítsem a fejlesztési folyamatot, így megállapíthattam elérhető célokat, amelyek jelentősen hozzájárultak a tervezett funkciók sikeres megvalósításához.

A tervezést és az alkalmazás implementálását két fő fázisra osztottam fel: az első fázisban a grafikus felhasználói felülettel (GUI) és a parancssoros interfésszel (CLI) rendelkező program tervezésére koncentráltam, amely a vevőkön fut. Ebben a fázisban figyelembe kellett vennem, hogyan gyűjthettem és feldolgozhatom az adatokat.

A GUI célja az volt, hogy tartalmazza az összes alapvető funkciót, amely egy snifferben található, és ugyanakkor egyszerű és intuitív legyen használni, létrehozva egy olyan felületet, amelyet a felhasználó könnyen megérthet és átláthat.

A második fázisban a térkép tervezésére összpontosítottam. Itt az már gyűjtött adatok alapján kellett kialakítanom a készülékek reprezentációját, ami magában foglalta a nagy mennyiségű adat feldolgozását, komplex matematikai számítások alapján.

A Raspberry Pi vevőkön futó parancssoros interfész programnak számos feladatot kellett ellátnia: keretek rögzítésének kezdése és befejezése, ezek mentése .pcap kiterjesztésű fájlba, és közben az Raspberry Pi-n futó operációs rendszer órájának szinkronizálása.

Ezenkívül a felhasználói felülettel rendelkező programnak képesnek kellett lennie arra, hogy megjelenítse a .pcap fájl tartalmát, a rögzített adatokat, térképet tudjon létrehozni, törölje a megjelenített adatok, valamint az elfogott adatokból kiszűrje az eszközöket. A térképet három célra terveztem:

1. Adatok feldolgozása
2. Az eszköz pozíciójának kiszámítása a feldolgozott adatok alapján
3. Navigálás a megjelenített időpillanatok között

A GUI a CLI verzió kiterjesztése, amelyet a vevőkön használtak, és ráadásul a térképnek saját modulja van, amit a GUI hívhat meg.

4. IMPLEMENTÁLÁS

A tervezést követte az implementáció mely, az egyik legfontosabb lépés volt a munkám elvégzésében, hisz dolgozatom ezen szakaszában valósul meg a már megtervezett program. Fontos volt, hogy az elkészített terveket követve a megfelelő módszerekkel, illetve technológiákkal dolgozzak, annak érdekében, hogy az alkalmazás sikeresen elkészüljön, valamint hatékonyan, hibamentesen működjön. Mivel az implementáció szorosan követi a tervezést, ez a folyamat is két fő részre osztható:

1. Az első részben a parancssoros felhasználói felülettel (CLI) és a grafikus felhasználói felülettel (GUI) rendelkező program implementációjával foglalkoztam.
2. A második részben a térkép implementációjának részleteivel foglalkoztam, ahol a tervezési szakaszban kidolgozott módszereket használtam a jelintenzitás átalakítására és a eszközök megjelenítésére a térképen.

Ezenkívül az implementáció volt az a szakasz, amikor az említett második fejezetben említett technológiákat használtam fel, így a projekt alapjául szolgáló technológiák a következők voltak:

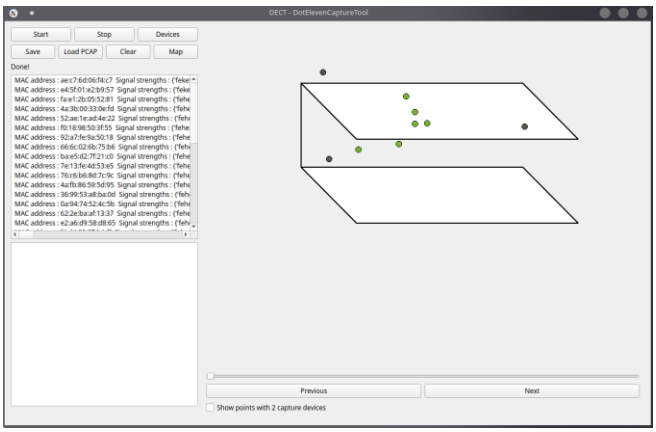
1. Python
2. Linux alapú operációs rendszer

A Python nyelvben kihasználtam azt, hogy létre tudok hozni osztályokat, így a különböző modulok szorosan összekötődnek annak ellenére, hogy különböző osztályokban vannak melyek egy úgy nevezett modul-ban helyezkednek el együtt, de mindegyiknek megvan a saját csomagja ezen a modulon belül is. Ez azt jelenti, hogy minden jól szét van választva, az objektum orientált programozás enkapszulációs elve szerint, azaz minden csak azt végzi el amire meg volt tervezve, és a további teendőket delegálja tovább egy specializálódott csomagnak.

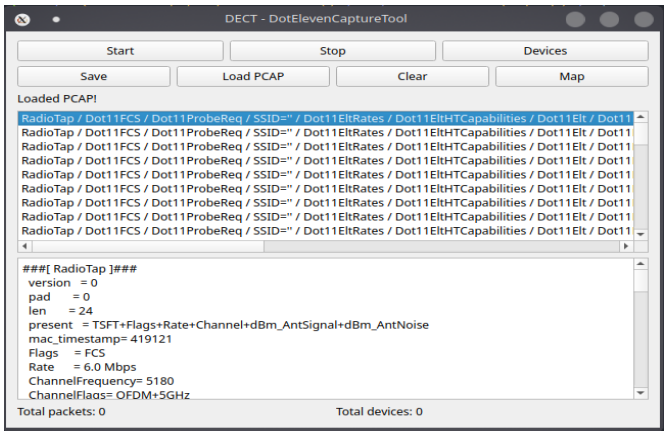
Az összes tervezett funkció megvalósításához különböző Python könyvtárakat használtam, amelyek segítettek az adatok feldolgozásában, a felhasználói felület megjelenítésében és a keretek gyűjtésében, ezek a könyvtárak a következőek voltak:

- MAC Vendor Lookup
- Numpy
- PyRIC
- PySide6
- Scapy
- Scipy
- CaptureInfos

Ezek segítségével sikerült megvalósítanom olyan funkciókat, mint a keretek rögzítése, a hálózati kártya manipulálása a monitor módba helyezéshez, valamint a PCAP fájlok feldolgozása a pozíció kiszámításához és a térkép rajzolásához. Ezek mellett sikerült megvalósítanom a grafikus felhasználói felületet is a fent említett könyvtárak segítségével.



1. ábra. Az adatokból készített térkép



2. ábra. Az alkalmzás betöltött adatokkkal

5. KÍSÉRLETEK

A kísérletezés a munkám befejezésének kritikus és végleges szakasza volt. Az kísérletek során adatokat gyűjtöttem, melyeket reprezentálni és elemezni tudtam, ezzel tesztelve nemcsak a vevőeszközök működését, hanem a térképet és a felhasználói felületet is. Az adatgyűjtés folyamata kiemelkedően fontos volt, mivel lehetővé tette az összes projekt komponensének tesztelését, kezdve a vevőeszközökkel.

A kísérletek jelentősen hozzájárultak a projekt megvalósításának sikeréhez, mivel számos optimalizációt eredményezett, amelyek növelték az alkalmazás hatékonyságát és sebességét. A különböző környezetek sokfélesége szintén fontos volt, mivel így biztosítani tudtam, hogy a programom megfelelően működik minden körülmények között. Ennek az előzőleg említett sokféleségnek köszönhetően három nagyon különböző helyen végeztem kísérleteket:

- A Marosvásárhelyi “George Emil Palade” Orvosi, Gyógyszerészeti, Tudomány és Technológiai Egyetem területén.
- Egy többszintes irodaházban.
- Egy magánházban.

Ez a három környezet jelentősen különbözött egymástól több szempontból is:

- A hálózati forgalom jelentősen eltért, mivel a készülékek és hozzáférési pontok száma változott.

- A fogadott jel minősége is változott, mivel a falak vastagsága és más zavaró tényezők eltérőek voltak ezekben a környezetekben.

Így képes voltam biztosítani, hogy a programom megfelelően működik bármilyen környezetben, és optimalizálhattam azt, hogy a felhasználó hatékonyan kezelhesse az adatok szűrését és reprezentációját.

Fontos megjegyezni, hogy a vevőeszközök csak azokat a kereteket fogadták, amelyeket a térkép képes volt feldolgozni, így a PCAP fájlok három fő kerettípust tartalmaznak:

- Probe Request
- Association Request
- Authentication Request

Kísérleteim több órán keresztül tartottak, és több száz vagy akár ezer keretet is begyűjtöttek, amiből sikeresen tudtam térképeket készíteni, és fontos következtetéseket vonhattam le, amelyek lehetővé tették számomra javaslatok kidolgozását.

6. KÖVETKEZTETÉSEK ÉS JAVASLATOK

A kísérletek fejezetben bemutatott eredmények alapján számos fontos következtetést vonhattam le és pár javaslatot is teszek az alkalmazás további fejlesztésére. Ebben a fejezetben összefoglalom ezeket a következtetéseket és javaslatokat, amelyek nem csak a jelenlegi kutatásom eredményeit értelmezik, hanem iránymutatást is adnak a projekt jövőbeli folytatásához.

Ami tisztán látszik a kísérletek eredményeiből, abból, hogy vevőnkként mennyire eltérő a begyűjtött adatmennyiség egyes helyzetekben az az, hogy fontos a vevőket optimálisan lehelyezni. Emiatt gondolom úgy, hogy fontos az elkövetkezendőkben a vevők helyének megfelelő megválasztása lehelyezéskor, ezáltal ki lehet küszöbölni azt, hogy a begyűjtött adat mennyiség drasztikusan eltérő legyen, mivel fontos az, hogy az adatok minél egységesebbek legyenek a lehető legoptimálisabb eredmények elérése érdekében.

Továbbá annak érdekében, hogy a térkép adatai még pontosabbak legyenek, fontos az, hogy a vevők órája szinkronizálva legyen. Itt két módszer is szóba jöhet, nevezetesen:

1. Az első módszer a beépített óra szinkronizálási módszer, amelyhez egy specifikus keret kiküldésére van szükség melyet a vevők feldolgoznak. Viszont annak ellenére, hogy a programom tartalmazza a módszert arra, hogy az órák szinkronizáljuk, mindezt nem tudtam végre hajtani, mivel nem volt megfelelő hálózati kártyám a keretek injektálására, nem tudtam elküldeni és elkészíteni ezáltal az óra szinkronizálási kereteket. Fontos, hogy a megfelelő hardvert használjuk ahhoz, hogy a szinkronizáló kereteket kiküldjük, ezáltal elkerülhetjük azt, hogy egyes vevők ne kapják meg az óra szinkronizálási keretet, mivel, ha a vevők órái szinkronizálva vannak, további funkciókkal lehet kiegészíteni az alkalmazás térkép részét, így precízebb eredményeket érhetünk el.
2. A másik módszer az lenne, hogy az alap hardver, amin a szoftver fut rendelkezzen azzal a lehetőséggel, hogy miközben monitor módban van fenn tudjon tartani egy olyan interfészt a hálózati kártyán, amely tud csatlakozni az internetre, így nem lenne szükség az óra szinkronizáló keretek kiküldésére, illetve feldolgozására.

Jövőbeliekben fontos lehet az is, hogy minél jobban automatizáljuk az alkalmazás működését. Jelenleg ahhoz, hogy az adatokat fel tudjuk dolgozni minden Raspberry PI-t külön el kell indítani és megszerezni róluk a PCAP fájlokat, ez időigényes lehet attól függően, hogy mekkora a fájl, illetve, hogy milyen erős a Raspberry PI, melyik verziót használtuk. Annak érdekében, hogy még jobban lehessen automatizálni a vevők és a feldolgozó közti kommunikációt ajánlott Raspberry PI 3 alapú vevőket használni vagy bármilyen olyan alap hardvert, amely rendelkezik azzal a lehetőséggel, hogy miközben monitor módban van fenn tudjon tartani egy olyan interfészt a hálózati kártyán, amely tud csatlakozni az internetre. Így fel tudná tölteni a kapott adatokat egy szerverre és el tudná küldeni az adott szerver címét a feldolgozó gépére, ezzel is lerövidítve a folyamat hosszúságát, illetve megkönnyítve azt.

Továbbá ajánlott az is, hogy minél több vevőt használjunk, legalább hármat vagy többet, akkor, ha az adatok alapján majd szeretnénk egy térképet készíteni. Ezt azért érdemes mert két vevő esetében nem tudunk pontosan kirajzolni egy térképet. Legalább három vevő szükséges a pontos helyzet meghatározásához, de minél több vevőt használunk annál pontosabb lesz az eszközök helyzetük a térképen és annál több eszközt tudunk észlelni is.

IRODALMI HIVATKOZÁSOK

[1] Lorenz Schauer, Florian Dorfmeister, and Florian Wirth, *Analyzing passive wi-fi finger-printing for privacy-preserving indoor-positioning*, 2016
[2] Shuang Shang and Lixing Wang, *Overview of wifi fingerprinting-based indoor positioning*, 2022
[3] Qiang Xu, Rong Zheng, Walid Saad, and Zhu Han, *Device fingerprinting in wireless networks: Challenges and opportunities*, 2015
[4] Sergey Bratus, Cory Cornelius, David Kotz, and Daniel Peebles, *Active behavioral finger-printing of wireless devices*, 2008