Литература

1. Захарченко Н.В. Пропускная способность канлов при таймерных сигнальных конструкциях / Н.В. Захарченко, М.М. Гаджиев, А.А. Русаловская // Матеріали XII міжнародної науково-технічної конференції ОНАЗ ім. О.С. Попова, Одеса. - 2013. - С. 186-188.

2. Захарченко Н.В. Оптимизация синдромного метода исправления ошибок в адаптивных системах / Н.В. Захарченко, М.М. Гаджиев, С.И. Лысенко, Д.В. Талакевич // Восточно-европейский журнал передовых технологий. -2013. - №5/2 (65) - С. 13-18.

3. Захарченко Н.В. Повышение эффективности блокового кодирования при работе по нестационарным каналам связи / Н.В. Захарченко, М.М. Гаджиев, С.В. Горохов та інші, загалом 7 осіб // «ЭЛМ». – Баку (Азербайджан), 2009. - 362 с.

References

1. Zaxarchenko N.V. Propusknaya sposobnost kanlov pri tajmernyx signalnyx konstrukciyax / N.V. Zaxarchenko, M.M. Gadzhiev, A.A. Rusalovskaya // materiali xii mizhnarodnoї naukovo-texnichnoї konferencії onaz im. O.S. Popova, Odesa. - 2013. - s. 186-188.

2. Zaxarchenko N.V. Optimizaciya sindromnogo metoda ispravleniya oshibok v adaptivnyx sistemax / N.V. Zaxarchenko, M.M. Gadzhiev, S.I. Lysenko, D.V. Talakevich // vostochno-evropejskij zhurnal peredovyx texnologij. -2013. - №5/2 (65) - s. 13-18.

3. Gaxarchenko N.V. povyshenie effektivnosti blokovogo kodirovaniya pri rabote po nestacionarnym kanalam svyazi / N.V. Zaxarchenko, M.M. Gadzhiev, S.V. Goroxov ta inshi, zagalom 7 osib // «elm». – baku (Azerbajdzhan), 2009. - 362 s.

Рецензія/Peer review : 9.11.2015 р. Надрукована/Printed :13.12.2015 р.

УДК 004.891

О.В. КЛІЩ
Хмельницький національний університет
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
Khmelnytsk national university
O.V. OHNIEVYI
Khmelnitsky national university, Ukraine

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

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.

Keywords: *Wi-Fi, access point, package, tracking.*

Вступ. Wi-Fi-технологія у наш час - це, насамперед, можливість отримувати доступ до нтернету без наявності будь-яких проводів. Все що потрібно для створення бездротової мережі – це точка доступу (або, як її ще називають, Wi-Fi роутер) і хоча б один клієнт, тобто підключений до неї комп'ютер або мобільний пристрій.

Той факт, що у всіх сучасних портативних девайсах реалізовані функції Wi-Fi, полегшує застосування цієї технології в публічних місцях. Вже зараз доступ у Всесвітню павутину через Wi-Fi став нормою для відвідувачів кафе і ресторанів, студентів різних навчальних закладів, постояльців готелів тощо. Увійти в бездротову мережу можна не тільки з комп'ютера або ноутбука, але і з мобільного телефону. Більшість користувачів за день підключаються до кількох точок доступу: вдома, на роботі, в кафе і т.д. Отож нашим завданням є визначення точок доступу до яких підключався користувач, та визначення їх географічного розташування. Існують й інші методи визначення місцеположення девайсу, та наше завдання здобути якомога більший список мереж, до яких користувач підключався, для отримання більшого об'єму

інформації про власника пристрою.

Постановка завдання. В процесі реалізації методу постає декілька основних завдань.

1. Перехоплення пакету
2. Аналіз вмісту пакету
3. Отримання карти підключень

Для перехоплення пакетів потрібен лише ПК із вбудованим або підключеним Wi-Fi адаптером, та встановленим спеціальним ПЗ. Оскільки ноутбук із адаптером для безпровідного з'єднання в наш час достатньо, залишається лише вибрати необхідне ПЗ. У виборі ПЗ слід спиратися, в першу чергу, на встановлену на ПК операційну систему.

Аналіз вмісту полягає у виборі необхідної нам інформації, та певної систематизації отриманих даних.

Останнє з головних завдань, що постають в процесі реалізації даного методу, полягає в перенесенні отриманих, з перехопленого пакету, даних на карту.

Основна частина. Аналізатор трафіку, або сніфер — програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів.

Перехоплення трафіку може здійснюватися:

- звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), інакше метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);
- підключенням сніфера в розрив каналу;
- відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;
- через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;
- через атаку на канальному (2) (MAC-spoofing) або мережевому (3) рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, із застосуванням лише простих засобів автоматизації, то він підходить для аналізу лише невеликих його обсягів. Нас це абсолютно влаштовує, оскільки ми будемо аналізувати трафік одного пристрою.

Для реалізації я використовував ноутбук укомплектований вбудованим Wi-Fi адаптером, із встановленою операційною системою "Windows 7". Проаналізувавши декілька сніферів я обрав Airodump-ng – аналізатор трафіку, котрий поміщає трафік у файли PCAP або ITT і показує інформацію про мережах.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54.  OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11e  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54   WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Rate    Lost    Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   36-24     2         14
(not associated)   00:14:A4:3F:8D:13   19    0-0      0          4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1   36-36     0          5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   54-54     0         99  teddy
```

Рис. 1. Приклад роботи аналізатора трафіку Airodump-ng

Як бачимо на рис.1. кожен з підключених пристроїв надсилай точці доступу багато пакетів, на що вказують цифри у колонці Packets. Але нас цікавлять пакети Probe request frame, оскільки прочитавши саме його ми отримаємо необхідну нам інформацію, а саме - ім'я мережі та mac-адресу пристрою.

З інформації на рис.2. ми отримали:

- MAC адреса пристрою - 50:ea:d6:aa:bb:cc;
- ім'я мережі – SUBWAY;

```
16:32:26.628209 BSSID:ff:ff:ff:ff:ff:ff DA:ff:ff:ff:ff:ff:ff SA:50:ea:d6:aa:bb:cc
    Probe Request (SUBWAY) [1.0 2.0 5.5 11.0 Mbit]
```

Рис. 2. Фрагмент пакету probe request

Таким чином ми отримали дані, з якими будемо далі працювати.

Існує чимало мереж зі розповсюдженими іменами, але в більшості будинків мережі будуть мати створені імена: модель роутера, провайдер та.ін.; або імена задані користувачем. Здавалося б що ця інформація нічого не дасть нам крім здогадок про місце роботи, провайдера. Але є такий ресурс як Wigle.

Wigle - це веб-сайт для збору інформації про різні точки доступу Wi-Fi по всьому світу. Користувачі можуть зареєструватися на сайті і завантажити дані точок доступу, такі як GPS-координати, SSID, MAC-адресу та тип шифрування, використані у виявлених хот-спотах.

Це сервіс, що працює під девізом «Всі мережі, які знаходять всі люди». І більшість міських мереж дійсно можна знайти в цьому сервісі. Більше того, що мережі, котрі цікавлять вас, ви можете знайти пошуком по їх назві. Саме так ви отримаєте інформацію про необхідні мережі за їх іменами. Можна зробити деякі припущення. наприклад, якщо Wigle повертає більше 3-4 мереж з однаковими іменами - це, швидше за все, якісь стандартні мережі, які можна ігнорувати, якщо тільки одна з них не знаходяться близько до тих унікальних, що ми знайшли. Можна відфільтрувати ті мережі, які не були видні більше року, якщо тільки вони не унікальні і не переміщалися в часі – інакше це буде означати, що точка доступу була переміщена.

Інформація про першу точку доступу була завантажена на Wigle у вересні 2001 року, а до серпня 2013 року у базі даних Wigle нараховувалось більше 107 млн. записів Wi-Fi мереж, з яких 105 млн. були записані із GPS координатами і зареєстровано понад 2 млрд. унікальних спостережень.

Але наше завдання зворотне – відштовхуючись від інформації отриманої з перехопленого пакету визначити географічне розташування мережі Wi-Fi.

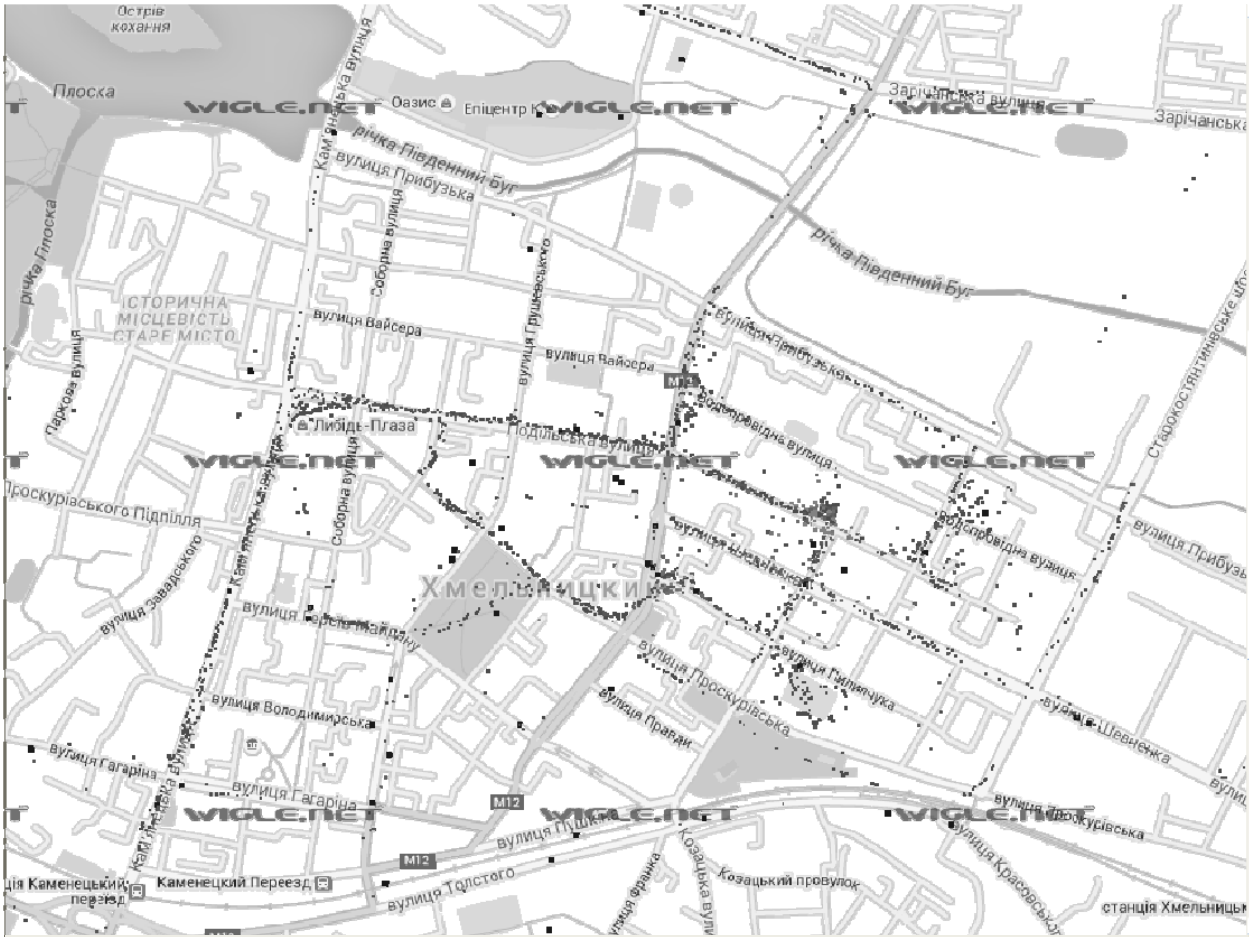

Рис. 3. Фрагмент карти Wi-Fi мереж м. Хмельницького

Висновки. Основною відмінністю та перевагою даного методу є відносна простота реалізації, і можливість отримання всієї необхідної інформації без контакту з досліджуваним пристроєм. Це дозволить використовувати його в умовах конфіденційності, що буде корисним для певних державних та приватних силових структур, і комерційних установ, які прагнуть дослідити переміщення своїх співробітників.

Поставлені основні задачі для реалізації описаного методу, проаналізовано можливі шляхи їх вирішення, та обрані найдоступніші та найефективніші з них. Повністю описана послідовність вирішення поставлених задач, та реалізації методу вцілому.

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.
5. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А. А. Владимиров, К. В. Гавриленко, А. А. Михайловский; пер. с англ. АА. Слинкина. — М.: НТ Пресс, 2005. — 463, с

References

1. Wi-Fi. (Wikipedia - the free encyclopedia) [Electronic resource]. – Режим доступу до статті: https://uk.wikipedia.org/wiki/Захист_у_мережах_Wi-Fi.
2. Dzhon Ross. Wi-Fi. Besprovodnaia set / Dzhon Ross ; per. s anh. V. A. Vetluzhskykh. – Moskva: NT Press, 2007. – 320 p.
3. Zakhyst u merezhakh Wi-Fi. (Wikipedia - the free encyclopedia) [Electronic resource]. – Режим доступу до статті: https://uk.wikipedia.org/wiki/Захист_у_мережах_Wi-Fi
4. Shcherbakov A. K. Wi-Fi: Vse, chto Vы khotely znat, no boialys sprosyt / Shcherbakov A. K.; - Moskva: LA «Buk-Press», 2005. - 352 p.
5. Wi-fu: “boevye” pryemy vzloma y zashchyty besprovodnykh setei / A. A. Vladymyrov, K. V. Havrylenko, A. A. Mykhailovskyi; per. s anhl. A. A. Slynkyna. - M .: NT Press, 2005. - 463, p.

Рецензія/Peer review : 6.11.2015 р. Надрукована/Printed :19.12.2015 р.

УДК 004.925.4

С.И. ВЯТКИН
Институт автоматики и электрометрии СО РАН, Новосибирск, Россия
А.Н. РОМАНЮК, А.А. ДУДНИК
Винницкий национальный технический университет, Украина

АНИЗОТРОПНАЯ ФИЛЬТРАЦИИ ТЕКСТУРЫ В РЕАЛЬНОМ ВРЕМЕНИ

Предлагается метод анизотропной фильтрации в режиме реального времени. Как более качественная альтернатива трилинейной фильтрации представлен метод приближения эллипса с большим эксцентриситетом несколькими эллипсами с меньшими эксцентриситетами для высокой степени анизотропии.
Ключевые слова: текстурирования, анизотропная фильтрация, фильтрация текстур.

S.I. VYATKIN
Institute of Automation and Electrometry SB RAS, Novosibirsk, Russia
O.N. ROMANYUK, O.O. DUDNYK
Vinnitsa National Technical University, Ukraine

THE METHOD OF ANISOTROPIC TEXTURE FILTERING IN REAL TIME

A method of anisotropic filtering in real time. As a higher quality alternative to tri-linear filtering approximation method presented an ellipse with an eccentricity of several large ellipses with eccentricities less for a high degree of anisotropy.
Keywords: texturing, anisotropic filtering, texture filtering

Введение

Применяемые в трехмерной графике методы наложения текстур, используются для визуализации трехмерных сцен с высокой степенью детализации. Генерация текстуры заключается в проецировании изображения на трехмерную поверхность, таким образом, обеспечивается дополнительная детализация объекта без усложнения его геометрии. При этом появляется множество разнообразных ошибок визуализации, называемых артефактами [1]. Было разработано множество различных методов, которые уменьшают количество подобных артефактов визуализации. Для имитации реалистичных сцен необходимо использовать большое количество детализированных текстур.

Поточечная выборка - самый простой метод определения цвета пикселя на основе текстурного изображения. Выбирается тексель, ближе всех расположенный к центру светового пятна. Вследствие того, что цвет пикселя определяют несколько текселей, а выбирается только один, происходит ошибка. Кроме того, форма светового пятна может измениться в зависимости от наклона грани по отношению к наблюдателю [2].

Главное преимущество данного метода фильтрации - это низкие требования к ширине полосы пропускания памяти, т.к. для определения цвета пикселя, нужно выбрать всего лишь один тексель из текстурной памяти. Главный недостаток - ухудшение качества изображений при приближении полигона к точке наблюдения, когда количество пикселей становится больше количества текселей. Кроме того,