Вченому секретарю
спеціалізованої вченої ради
Д 64.052.03
Харківського національного
університету радіоелектроніки,
проф. Безруку В.М.
пр. Науки,14, м. Харків, 61166

ВІДГУК

офіційного опонента
доцента кафедри безпеки інформаційних систем і технологій
Харківського національного університету імені В. Н. Каразіна
Нарєжнього Олексія Павловича
на дисертаційну роботу **Василенко Тетяни Олександрівни** на тему
"**Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі**", яка подана
на здобуття наукового ступеня кандидата технічних наук за спеціальністю
05.12.17 – радіотехнічні та телевізійні системи

Актуальність дисертаційних досліджень

Захищеність Wi-Fi мереж забезпечується з допомогою двох основних методів, що закладені в алгоритм їх роботи: це ідентифікація користувачів при доступі до мережі та криптографічний захист даних, що передаються.

Криптографічний захист, що застосовується для шифрування в Wi-Fi мережах, дійсно захищає дані, але має свої вразливості. Відомо, що для усунення вразливостей в протоколах WEP, WPA мережі Wi-Fi був запропонований протокол WPA2. Використання в WPA2 блочного симетричного шифру AES-128 (FIPS 197) в режимі лічильника з CBC-MAC (режим CCM), з явною ініціалізацією вектору (IV) надає наступні послуги безпеки: конфіденційність і цілісність даних, ідентифікацію, контроль доступу в поєднанні з керуванням рівнів. Режим CCM протоколу потребує використання нових тимчасових ключів для кожної нової сесії. Для генерації криптографічного ключа застосовується схема 4-way-handshake. У моделі загроз передбачається, що зловмисник може «прослуховувати» Wi-Fi трафік, здійснювати атаки типу «людина посередині» і атаки типу спуфінг.

До 2017 року основними методами злому WPA2 PSK були атака «грубої сили» і атака за словником. Для цього порушник в режимі моніторингу сканує ефір і записує необхідні пакети. У жовтні 2017 року

була опублікована атака з переустановкою ключа (англ. KRACK, Key Reinstallation Attack), основана на ряді вразливостей при реалізації схеми 4-way-handshake.

У 2018 році для усунення знайдених вразливостей протоколу WPA2 мережі Wi-Fi був анонсований новий протокол бездротового безпеки WPA3. При цьому контроль доступу на фізичному рівні моделі (OSI) при протидії атакам типу спуфінг продовжує залишатися актуальною науковою задачею.

Робота, направлена на захист Wi-Fi мереж від спруфінг атак шляхом врахування індивідуальних ознак пристроїв мережі на фізичному рівні, є актуальною і сприятиме підвищенню захищеності мережі.

Аналіз змісту дисертаційної роботи

Основні структурні елементи дисертації, а також її оформлення відповідають вимогам Наказу № 40 від 12.01.2017 р. Міністерства освіти і наук України «Про затвердження вимог до оформлення дисертації». Дисертаційна робота викладена на 145 сторінках і складається із вступу, чотирьох розділів, висновків, списку використаних джерел, у який включено 82 найменувань та додатків, у який включено 3 акти впровадження результатів дослідження. У роботі наведено 48 рисунків і 17 таблиць.

У вступі наведено загальну характеристику дисертації, сформульовано мету, науково-прикладну задачу, завдання, об'єкт і предмет дослідження, які відповідають темі дисертації.

У розділах дисертації повно і вичерпно викладено зміст власних досліджень. Організація матеріалу дисертації за розділами є логічною.

В першому розділі дисертаційної роботи розглянуто загрози та вразливості властиві Wi-Fi мережам. Зроблено огляд способів їх захисту від несанкціонованого доступу з виявленням недоліків та вразливостей таких систем. Зокрема, зроблено огляд систем шифрування від протоколу WEP до WPA3, де вказано на їх вразливості та методи злому. На початку 2018 року був анонсований новий протокол WPA3, а вже в наступному 2019 році з'явилися публікації про комплекс проблем, що отримав ім'я DragonBlood – «в честь» вразливого Dragonfly механізму, за допомогою якого клієнти проходять ідентифікацію на пристроях з підтримкою нового стандарту WPA3. В DragonBlood об'єднані п'ять вразливостей, включаючи відмову в обслуговуванні, дві проблеми, що призводять до side-channel витокам, і ще дві проблеми, пов'язані з даунгрейдом з'єднань. В результаті DragonBlood дозволяє атакуючому, що знаходиться в зоні доступу Wi-Fi мережі, відновити паролі жертви і проникнути в мережу.

Другий розділ дисертації присвячено розробці нового методу ідентифікації пристроїв Wi-Fi, що оснований на відомих прийомах радіомоніторингу але вперше був застосований для задач захисту Wi-Fi мереж. Проведено експериментальні дослідження з отримання спектральних характеристик пристроїв абонентів бездротової мережі. Показано, що вони мають свої індивідуальні особливості, які можуть бути використані як ідентифікуюча ознака. Причому спектри різних пристроїв мають суттєві відмінності, а для одного й того ж пристрою в різних положеннях, відносно приймальної антени, спектр майже не відрізняється – більшою мірою змінюється рівень сигналу. Шляхом усереднення спектральних характеристик пристрою в різних положеннях були отримані шаблони спектрів для кожного з них, які мають зберігатися в базі даних системи захисту. В розробленому алгоритмі пропонується проводити перевірку пристроїв користувачів мережі порівнюючи реальній поточний спектр з його шаблоном.

Також в другому розділі розроблено два методи обробки спектральних характеристик для їх порівняння. Перший полягає в обчисленні середнього квадрату різниць всіх спектральних складових, що підлягають перевірці з його шаблоном. Другий – в обчисленні коефіцієнта асиметрії по взаємокореляційним функціям пристрою з шаблоном.

В третьому розділі дисертації запропоновано використовувати місцеположення абонентів бездротової мережі, як одну з ознак для виявлення підозрілого стану мережі. Для реалізації даного методу пропонується використовувати вже присутні в мережі точки доступу, що зв'язані між собою, котрі спілкуючись з абонентами будуть передавати дані про їх рівень сигналу для системи захисту. В розділі були проаналізовані існуючі системи визначення місцеположення та зроблено висновок, що найбільш достовірну інформацію за умови розташування таких систем в приміщенні, де на рівень сигналу впливають безліч перешкод, можна отримати шляхом побудови радіокарт приміщення. Для перевірки похибки в визначенні місцеположення були проведені експериментальні дослідження, які виявили, що похибка даного методу може складати 2,5 метри, що можна порівняти з існуючими комерційними системами позиціонування.

У четвертому розділі дисертації була створена математична модель шуму та імітації його додавання з експериментально отриманими спектральними характеристиками. Проведене моделювання дозволило оцінити ймовірнісні характеристики запропонованого методу ідентифікації користувачів мережі в різних умовах, що для реального експерименту було б складно.

Отримані графіки залежності середніх квадратів різниці та коефіцієнтів асиметрії пристроїв по відношенню до різних шаблонів. Показано, що при порівнянні спектрів по середньому квадрату різниць розпізнавання спектрів безпомилково зберігається до відношення сигнал/шум 25 дБ, при такому, або більшому відношенні сигнал/шум зазвичай і працює бездротова мережа. При зменшенні відношення сигнал/шум, починають виникати помилки. При порівнянні спектральних характеристик по коефіцієнту асиметрії, пристрої різних моделей однозначно розрізняються навіть при відношенні сигнал/шум 10 дБ.

У висновках по роботі міститься формулювання розв'язаної науково-прикладної задачі, викладені найважливіші наукові та практичні результати, одержані в дисертації.

Дисертація за змістом та отриманими результатами відповідає паспорту спеціальності 05.12.17 – радіотехнічні та телевізійні системи, зокрема п. 2 – дослідження методів оптимізації систем і комплексів, пристроїв, вузлів, формування й обробка сигналів в умовах реальної завадової обстановки, та п.5 – синтез і аналіз систем виявлення, вимірювання параметрів сигналів, адаптація їх до змін зовнішнього середовища та джерел інформації.

Зміст автореферату відповідає основним положенням дисертації.

Ступінь обґрунтованості наукових положень в дисертації

Обґрунтованість отриманих в дисертації експериментальних результатів підтверджуються тим, що:

– для дослідження використовувалося достатня кількість різних пристроїв;

– отримані результати для всіх пристроїв повністю вкладаються в маску спектральної щільності, визначену стандартом;

– для всіх вимірювань дотримувалися однакові умови;

– за результатами вимірювань спостерігалася схожість спектрів для різних положень одного й того ж пристрою та ідентичність спектрів для одного і того ж пристрою при повторних вимірах.

Обґрунтованість отриманих в дисертації теоретичних висновків обумовлена коректним використанням математичних методів і методів моделювання та підтверджуються схожістю результатів ідентифікації різними розрахунковими методами.

Наукова новизна результатів дисертації

До наукових результатів дисертаційної роботи Василенко Т.О. можна віднести наступне:

1. Розроблено новий метод ідентифікації абонентів бездротових мереж, оснований на використанні особливостей спектральних характеристик пристроїв абонентів Wi-Fi мереж, що відрізняється від вже відомих областю застосування, а саме використання спектральних особливостей пристроїв для захисту від спуфінг атак.

2. Розроблено новий метод обробки енергетичного спектру сигналу, який дозволяє порівнювати шаблонний та поточний спектри пристроїв, шляхом розрахунку середнього квадрату різниці їх складових. На відміну від існуючих методів, що основані на розрахунках середнього квадрата різниці, даний метод дозволяє не просто класифікувати спектри на класи випромінювань але й дозволяє виявити розбіжності в спектрах одного класу (Wi-Fi випромінювання).

3. Розроблено новий метод обробки енергетичного спектру сигналу по коефіцієнту асиметрії взаємокореляційних функцій, що на відміну від відомих методів, дозволяє однозначно розрізняти різні пристрої при мінімальному відношенні сигнал/шум.

4. Вперше запропоновано використовувати місцеположення пристроїв абонентів в системах виявлення вторгнень, як одну з ознак, що дозволяє захистити Wi-Fi мережі від спуфінг атак.

5. Розроблено нову модель, що імітує шумову обстановку в бездротовій мережі, для перевірки працездатності розроблених методів в реальних умовах функціонування.

Практична значимість роботи

Практична значимість роботи визначається наступними результатами:

1. В роботі було виявлено, що спектральні характеристики одного й того ж пристрою в різних положення не мають великих відмінностей, в той час як спектральні характеристики різних пристроїв суттєво відрізняється й можуть бути використані для ідентифікації абонентів мережі.

2. Було розроблено та експериментально перевірено методику визначення місцеположення з точністю 2.5 м, для врахування місцеположення абонентів, при виявленні нідозрілої активності в бездротовій мережі.

3. Розроблений алгоритм врахування індивідуальних ознак фізичного рівня пристроїв бездротової мережі, що не враховуються в існуючих системах захисту Wi-Fi, що дозволяє підвищити безпеку в цих мережах.

4. Результати моделювання по додаванню шуму до експериментальних спектрів показують, що при погіршенні відношення сигнал/шум до 25 дБ ймовірність помилки ідентифікації менше 1%, при

20 дБ – 20%. (Практично передача даних в Wi-Fi відбувається при відношенні сигнал/шум до 25 дБ).

5. Результати дисертаційної роботи прийняті до використання виробничим підрозділом «Харківське відділення» філії «Головний інформаційно-обчислювальний центр» АТ «Укрзалізниця» при аналізі стану захищеності інформаційних ресурсів для підвищення безпеки систем бездротового, про що є відповідній акт впровадження.

6. Матеріали дисертаційної роботи використовуються в освітньому процесі Харківського національного університету радіоелектроніки на кафедрі комп'ютерної радіоінженер та систем технічного захисту інформації в курсі лекцій з дисципліни «Обробка сигналів в системах ТЗІ» і при підготовці магістерських атестаційних робіт, про що є відповідній акт впровадження.

Апробація роботи

Результати дисертаційних досліджень Василенко Т.О. пройшли апробацію на 8 міжнародних наукових конференціях, а також достатньо повно викладені у 7 статтях у фахових виданнях, затверджених МОН України. Одна із цих статей опублікована у виданні, що входить до наукометричної бази Scopus.

Недоліки та зауваження до дисертаційної роботи

1. Було б доцільно доповнити дисертаційну роботу моделлю загроз та моделлю порушника.

2. У четвертому розділі дисертаційної роботи, де на рисунку 4.7 та 4.10 наведені залежності ймовірності помилкової тривоги і пропуску цілі від установленого порогу для різних співвідношень сигнал/шум не вистачає текстового опису отриманих результатів.

3. Термін «помилкова точка доступу» не цілком відповідає суті атаки, яка англійською називається «fake access point». Більш коректно було б назвати підробна або фальшива точка доступу.

4. Оскільки ряд атак на бездротові мережі передбачає установку вищеназваних fake access point, то логічно було б провести дослідження і за їхніми спектрами випромінювання, а не тільки за спектрами випромінювання абонентських пристроїв.

5. На рисунке 4.7 (сторінка 118) присутня друкарська помилка, два нижні графіки залежності ймовірності помилкової тривоги і пропуску цілі від встановленого порогу абсолютно різні, а підписані однаково.

Зазначені недоліки не є принциповими і тому не впливають на загальну позитивну оцінку виконаної роботи, що характеризується цілком достатнім рівнем наукової новизни, де гарно відомі методи

радіомоніторингу застосовуються в нетиповому для даного поняття напрямку – забезпечення безпеки бездротових мереж.

Загальний висновок щодо дисертації

В цілому зауваження, які були виявлені у дисертаційній роботі, не ставлять під сумнів наукову та практичну значимість дисертаційної роботи Василенко Т.О. Дисертація є завершеним науковим дослідженням, в результаті якого вирішена актуальна науково-прикладна задача підвищення захищеності бездротової Wi-Fi мережі шляхом обґрунтованого врахування ознак її стану на фізичному рівні.

Вважаю, що дисертаційна робота Василенко Т.О. на тему "Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі" повністю відповідає вимогам пп. 9, 11 «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України, а її автор – Василенко Тетяна Олександрівна – заслуговує присудження їй наукового ступеня кандидата технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи.

Офіційний опонент
доцент кафедра безпеки
інформаційних систем і технологій
ХНУ імені В. Н. Каразіна,
кандидат технічних наук / Нарєжній О. П./

ПІДПИС ЗАСВІДЧУЮ
Начальник відділ
кадрів

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В.Н. КАРАЗІНА * КОД 02071205