МІНІСТЕРСТВО ОБОРОНИ
УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ ПОВІТРЯНИХ СИЛ
імені ІВАНА КОЖЕДУБА
код 24980799

«20» 04 2021 р.
№ 350/1770/21-276/311нс
61023, м. Харків, вул. Сумська 77/79

Вченому секретарю
спеціалізованої вченої ради
Д 64.052.03
Безруку В.М.
просп. Науки, 14, м. Харків,
61166

ВІДГУК

офіційного опонента, начальника науково-дослідної лабораторії факультету радіотехнічних військ протиповітряної оборони Харківського національного університету Повітряних Сил ім. Івана Кожедуба доктора технічних наук, старшого наукового співробітника **Костирі Олександра Олексійовича,** на дисертаційну роботу Василенко Тетяни Олександрівни на тему "Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі", яку подано на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи

Актуальність теми дисертаційної роботи

Аналіз сучасних досліджень показує, що до 2030 року кількість пристроїв Wi-Fi (Інтернету речей) виросте до 125 мільярдів. Значну частину Wi-Fi мережі будуть займати стаціонарні пристрої, що використовуються в банках, державних і військових установах. Тому радіомоніторинг пристроїв користувачів бездротових Wi-Fi мереж може бути одним з додаткових ознак для виявлення несанкціонованого доступу та атак зловмисників.

Методи розпізнавання (ідентифікації) джерел радіовипромінювання за часовими та частотними особливостям їх сигналів давно застосовуються в системах радіомоніторингу і радіотехнічної розвідки. Однак задача забезпечення безпеки Wi-Fi мереж є складною, багаторівневою, багатофакторною. Для її вирішення потрібне застосування допоміжних методів аналізу за рахунок розширення метрик, що розглядаються при визначенні несанкціонованого доступу, які є специфічними безпосередньо для Wi-Fi мереж.

В якості основних механізмів захисту Wi-Fi мереж від несанкціонованого доступу є шифрування та системи виявлення вторгнень. Відомі системи виявлення вторгнень (англ. WIDS - Wireless Intrusion Detection System) корпоративної Wi-Fi мережі – це системи, які збирають інформацію з різних точок і аналізують цю інформацію для виявлення не тільки спроб, а і реальних порушень захисту (вторгнень).

Перспективним напрямком є розробка гібридних моделей WIDS з системами радіомоніторингу, які об'єднають в собі сильні сторони обох

систем та підвищують захищеність корпоративної Wi-Fi мережі. Система радіомоніторингу повинна вирішувати задачу виявлення аномалій (Anomaly Detection) на фізичному рівні моделі OSI (Open System Interconnection) шляхом врахування індивідуальних ознак пристроїв (спектральних характеристик сигналу і місцеположення) та метрик визначення аномалій.

Тому науково-прикладну задачу ідентифікації Wi-Fi пристроїв шляхом врахування ознак фізичного рівня корпоративної мережі (спектральних характеристик сигналів, місцеположення пристроїв та метрик визначення аномалій) з метою підвищення їх безпеки слід вважати **актуальною**.

Зв'язок дисертаційних досліджень з державними наукових програмами та пріоритетними напрямками розвитку науки і техніки

Дисертаційні дослідження проводилися в рамках виконання планової НДР ХНУРЕ № 260-5 «Розробка методів моделювання інформаційних мереж, побудованих на основі реконфігурованих антен» (№ ДР 011U002903) , в якій здобувач була виконавцем.

Результати дисертаційних досліджень впроваджені у вказаній НДР, в Акціонерному товаристві «Укрзалізниця», а також в освітньому процесі кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації ХНУРЕ (в курсі «Обробка сигналів в системах ТЗІ»).

Наукова новизна отриманих результатів

У якості нових результатів дисертаційної роботи слід відзначити наступні:

1 Вперше запропоновано метод ідентифікації Wi-Fi пристроїв за спектрами випромінюваних їх сигналів, що полягає в порівнянні спектральних характеристик з шаблонними та сприяє перевірці достовірності ідентифікації за MAC-адресою. На відміну від відомих методів, ідентифікація пристроїв проходить як за стандартними параметрами автентифікації, так і за спектрами їх випромінювань.

2. Запропоновано два методи обробки спектральних характеристик Wi-Fi пристроїв, призначених для визначення ступеня відмінності між ними. Перший метод полягає в обчисленні середнього квадрата різниці, а другий – в знаходженні коефіцієнтів асиметрії взаємокореляційних функцій спектральних відліків аналізованого пристрою і шаблону. Відомі методи середнього квадрата різниці розділяють тільки спектри, що суттєво відрізняються, а для спектрів, які є досить подібними, не працюють. Метод обчислення коефіцієнту асиметрії взаємокореляційних функцій на відміну від відомих методів, однозначно розрізняє різні пристрої при погіршенні відношення сигнал/шум до 10 дБ.

3. Одержав подальший розвиток метод виявлення атак, оснований на виявленні місцеположення пристроїв мережі, що полягає у використанні методу радіовідбитків. Наявність інформації про місцеположення пристроїв спільно з системою виявлення вторгнень дозволяє виявляти і запобігати ряду атак на Wi-Fi мережі.

4. Розроблено нову модель процесу прийому Wi-Fi сигналу, що відрізняється урахуванням реальних шумових умов та дозволяє аналізувати

можливості ідентифікації Wi-Fi пристроїв при різних відношеннях сигнал/шум.

Практичне значення результатів роботи

1. Експериментально встановлено, що спектри випромінювання різних Wi-Fi пристроїв незалежно від положення мають значно більшу відмінність, ніж відмінність між спектрами випромінювання одного і того ж пристрою в різних положеннях, що може бути використано для ідентифікації пристроїв.

2. Розроблено методику визначення місцеположення абонента бездротової мережі за рівнем потужності випромінюваного сигналу з використанням методу радіовідбитків. Показано, що похибка у визначенні місцеположення становить 2,5 м при застосуванні детермінованого (евклідова відстань) підходу визначення координат в закритому приміщенні.

3. Запропоновано алгоритм аналізу стану Wi-Fi мережі, який дозволяє більш зважено приймати рішення про аномальний стан мережі шляхом врахування ознак, які не враховуються в діючих системах виявлення вторгнень.

Аналіз змісту дисертаційної роботи

Зміст дисертації, повнота викладення матеріалу, науковий рівень, порядок оформлення відповідають діючим вимогам до дисертацій на здобуття наукового ступеня кандидата технічних наук.

Дисертація складається із вступу, 4 розділів, висновків і додатків. Графічний матеріал підготовлено якісно і він добре доповнює зміст роботи.

Стиль викладення матеріалу дисертації чіткий та ясний.

Тематика дисертаційних досліджень відповідає паспорту спеціальності 05.12.17 – радіотехнічні та телевізійні системи.

Повнота викладення результатів дисертації в опублікованих роботах

За темою дисертаційної роботи опубліковано 7 наукових статей в фахових виданнях України, з яких одне видання входить до наукометричної бази Scopus. Основні положення роботи повністю розкрито в цих публікаціях.

Основні положення та висновки дисертації апробовано під час міжнародних науково-технічних форумів і конференцій, всього видано 8 тез доповідей на цих заходах.

Кількість публікацій та повнота відображення в них результатів досліджень відповідають вимогам до оформлення кандидатських дисертацій.

Обґрунтованість і достовірність наукових результатів

Обґрунтованість наукових результатів, отриманих в роботі, обумовлена наступним.

На етапі отримання експериментальних даних:

– використанням вимірювальної техніки відповідного діапазону частот і рівня точності для зняття спектральних характеристик;

– використанням програмного забезпечення, що додається до вимірювальної техніки, для первинної обробки та фіксації результатів вимірювань;

– дотриманням ідентичності умов при знятті спектральних характеристик різних Wi-Fi пристроїв;

– узгодженістю отриманих експериментальних і теоретичних даних.

На етапі обробки даних:

– коректним використанням математичного апарату при обчисленні середніх квадратів різниці та взаємних кореляційних функцій;

– адекватністю моделювання сигналів та перешкод при аналізі ефективності запропонованих методів в реальних умовах.

Можливість використання отриманих наукових та практичних результатів

Результати дисертаційної роботи Василенко Т.О. можуть бути використані при проведенні заходів з підвищення захищеності Wi-Fi мереж.

Зацікавленими у використанні результатів дисертаційних досліджень можуть бути:

- Міністерство оборони України;
- державні та комерційні фінансові установи;
- спеціалізовані наукові та проектні організації, які займаються розробкою систем технічного захисту інформації.

Відповідність змісту автореферату основним положенням дисертації

Автореферат відповідає змісту дисертаційної роботи, результати досліджень повністю відображені в публікаціях. Їхня кількість, повнота висвітлення результатів досліджень повністю відповідають установленим вимогам.

Недоліки та зауваження

Дисертаційна робота Василенко Т.О. виконана на високому рівні, однак вона має ряд недоліків.

1. Було б доцільно провести аналіз досліджуваних спектральних характеристик для більшої кількості пристроїв. Наведеної кількості пристроїв (п'ять) занадто мало для того, щоб стверджувати, що знайдені числові значення середнього квадрату різниці, коефіцієнтів асиметрії та порогів є остаточними і можуть бути перенесені на будь-яку іншу кількість пристроїв або на інші їх екземпляри.

2. Як відомо, в Wi-Fi мережах можуть застосовуватися різні види модуляції, в результаті яких можуть формуватися різні спектри. Але в роботі про види модуляції згадується лише раз в оглядовій частині підрозділу 1.1, а при експериментальних дослідженнях і аналізі їх результатів про ці відмінності нічого не вказано.

3. Автор залишає поза увагою питання про те, чим можуть бути викликані отримані відмінності в спектрах пристроїв мережі. Більш детальне дослідження таких відмінностей дозволило б сказати, наскільки стійкими є виявлені розбіжності в спектрах і в якій мірі їх можна намагатися імітувати.

4. На рис. 4.7 (с. 118) для двох різних графіків зазначено одне й те ж відношення сигнал/шум (імовірно помилково).

5. Мають місце орфографічні, стилістичні помилки та відхилення в оформленні:

- на стор. 66 замість терміну «математичне сподівання» слід застосовувати термін «математичне очікування»;

- на стор. 85 крайній рядок замість слова «одним» слід написати «одною»;

- у змісті дисертації та за текстом роботи вказані «Висновки до розділу 3», «Висновки по розділу 4», а слід застосовувати «Висновки за розділом…»;

- не дотримано інтервалів між назвою і текстом підрозділів (3.2.2, 4.1.2).

Вказані зауваження не є принциповими і не впливають на загальну високу позитивну оцінку виконаної роботи.

Загальні висновки

Дисертація Василенко Т.О. є завершеною науковою працею, в результаті якої вирішена актуальна наукова задача підвищення захищеності бездротової Wi-Fi мережі шляхом обґрунтованого врахування ознак її стану на фізичному рівні.

Задачі дослідження, положення наукової та практичної новизни, висновки та рекомендації достатньо обґрунтовані та аргументовані.

Дисертаційна робота відповідає вимогам "Порядку присудження наукових ступенів", затвердженою Постановою Кабінету Міністрів України, а здобувачка Василенко Т.О. заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи.

Офіційний опонент
Начальник науково-дослідної лабораторії факультету радіотехнічних військ протиповітряної оборони Харківського національного університету Повітряних Сил імені Івана Кожедуба
доктор технічних наук, старший науковий співробітник

Олександр КОСТИРЯ

20 квітня 2021 р.

Особистий підпис доктора технічних наук, старшого наукового співробітника Костирі Олександра Олексійовича засвідчую.

ТВО заступника начальника Харківського національного університету Повітряних Сил з наукової роботи
доктор технічних наук, старший науковий співробітник

Дмитро КАРЛОВ

20 04 2021 р.