УДК 004.65:620.92
DOI: 10.31673/2409-7292.2020.023746

Дубровін В.І., Петрик Б. В., Неласа Г.В.

ВИЯВЛЕННЯ DOS-АТАК В МЕРЕЖЕВОМУ ТРАФІКУ МЕТОДОМ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Аналіз даних мережевого трафіку дуже важливий для виявлення DOS-атак і шкідливої аномалії . Було знайдено багато методів інтелектуального аналізу даних, щоб управляти даними і використовувати їх в цілях безпеки. Швидкий і точний пошук за запитами на основі контенту вкрай важливий для того, щоб такі численні потоки даних були корисні. У цій статті пропонується аналіз атаки деавтентифікації та локалізація даних аномалії методом вейвлет-перетворення..

Ключові слова: Linux, вейвлет–перетворення, шумозниження, мережевий трафік, DOS-атака, ін'єкція пакетів, точка доступу.

Вступ

Сучасні мережеві системи (МС) розвиваються стрімко і набирають потужність. Компанії і організації, що використовують МС які налічують велику кількість комп'ютерів, першочерговим завданням вважають управління безліччю різноманітних захисних механізмів. Складність інфраструктури МС призводять до того, що при реалізації системи інформаційної безпеки за межами уваги адміністратора безпеки можуть залишитися багато вторгнень. Число інцидентів, пов’язаних з інформаційною безпекою, за даними провідних аналітичних агентств, постійно зростає.

Сьогодні досить рідко використовується атака DoS (Denial of Service), порівняно з розподіленою (або масивною) кібератакою на відмову в обслуговуванні - DDoS (Distributed Denial of Service), бо її набагато складніше відфільтрувати, а потужність може досягати до 1 Tbps. Однак саме схема DoS - основа сучасних кібератак на відмову в обслуговуванні. Значення атак DoS не варто недооцінювати - саме на них тренуються початківці зловмисники, і такі випадки вкрай рідко розслідуються. В результаті багато організацій і компаній не беруть до уваги потенційний вплив атаки типу DoS [1].

Вейвлет-перетворення(ВП) на сьогоднішній день є однією з найбільш перспективних технологій аналізу даних, його інструменти знаходять застосування в самих різних сферах інтелектуальної діяльності[2]. На відміну від перетворення Фур'є, вейвлет-аналіз дозволяє виділяти одночасно як частотну, так і часову компоненти мінливості, тобто дає можливість аналізувати часову мінливість частотного спектра процесу. Вейвлет-перетворення має рухоме частотно-часове вікно, яке самостійно налаштовується [3], однаково добре виявляє як низькочастотні так і високочастотні характеристики сигналу на різних часових масштабах. Вейвлет-фільтри дозволяють не тільки боротися з шумами, але і витягувати необхідні компоненти сигналу. Оскільки вейвлети мають гарну частотно-часову адаптацію, вони можуть служити зручним інструментом для дослідження частотних характеристик нестаціонарного сигналу [4], уявлення мережевого трафіку в різних масштабах. Перевага такого підходу - характерні деталі, які можуть залишатися непоміченими при одному масштабі, легко можуть бути виявлені на іншому рівні аналізу.

Постановка задачі. На сьогоднішній момент часу посилюються вимоги до якіснішого виявлення внутрішніх закономірностей в поведінці часових послідовностей і прогнозуються періоди стійкості досліджуваних процесів. Тому виникає необхідність в розробці нових і модифікації існуючих алгоритмів аналізу аномалії в мережевих системах.

В роботі досліджено особливості атаки девантентифікації в бездротовій мережі стандарту 802.11 та застосування ВП для виявлення DoS та DDos атак.

Виклад основного матеріалу

1. Особливості атаки деавтентифікації

Можливість реалізації атаки деавтентифікації безпосередньо пов’язана з особливостями механізму встановлення зв’язку в бездротовій мережі стандарту 802.11[5]. З'єднання між клієнтом та точкою доступу (ТД) встановлюється шляхом обміну різними кадрами, щоб

пройти процедури автентифікації і асоціації. Вразливе місце в процесі з'єднання (роз'єднання) пристроїв зосереджено під час відправки користувачем кадра деавтентифікації (deauth) Wi-Fi.

В[6] продемонстровано практичну реалізацію спеціального типу атаки - «відмова в обслуговуванні» Denial of Service (DoS) в мережах на основі стандарту 802.11. Дане дослідження ілюструє можливу схему дії зловмисника і сценарій атаки на клієнта.

Дослідження[7] дозволить продемонструвати можливу схему дії зловмисника і ситуацію атаки на клієнта. Результатом експерименту є метод отримання необхідної інформації про досліджувану систему під час атаки.

Суть атаки буде полягати в безперервній відправці пакетів деавтентіфікації одному або більше клієнтам Wi-FI мережі через що жертви не зможуть працювати в цій мережі. Для реалізації знадобитися операційна система Kali Linux. Існує безліч програм під Linux, для створення DoS-атаки, але в даному випадку буде використана утиліта AIrcrack-ng.

1.1 Концепція атаки

Стандарт Wi-Fi IEEE 802.11 вимагає виконання двох обов'язкових послідовних кроків до того, як користувач зможе почати передачу даних: автентифікація і асоціація. Тому, клієнт Wi-Fi може перебувати в будь-якому з 3 станів:

стан 0: клієнт не автентифікований і не асоційований;

стан 1: клієнт автентифікований, але не асоційований;

стан 2: клієнт автентифікований і асоційований.

В бездротовій мережі стандарту 802.11 з'єднання між клієнтом та точкою доступу (ТД) встановлюється шляхом обміну різними кадрами [8], але користувач зможе почати передачу даних тільки с 2 стану.

Пристрій користувача відправляє кадр деавтентифікації (deauth) Wi-Fi до іншого пристрою, коли хоче закінчити безпечне з'єднання. Коли клієнт отримує кадр deauth, він безпосередньо переходить в стан 0 незалежно від стану, в якому він знаходиться в даний момент. Отже, зловмисник може запустити атаку DoS, підробивши це повідомлення і тим самим відключивши зв'язок між бездротовими пристроями і їх точкою доступу. У разі, якщо атака буде продовжена, клієнт, безумовно, не зможе підключитися до бездротової мережі, поки зловмисник не скасує атаку [9]. Таким чином, при атаці DoS, коли зловмисник відправляє велику кількість кадрів deauth, клієнт, на якого націлена атака, досягає стану 0 і потребує повторної автентифікації, і повторного асоціювання. Тому, атака DoS є критичною атакою, яка порушує поточне завантаження і транзакцію, що виконується клієнтом.

1.2 Реалізація атаки в операційній системі Linux

Для проведення атаки потрібно перевести карту Wi-Fi в режим моніторингу. В цьому режимі апаратний інтерфейс не підключається до жодної мережі. Інтерфейс отримує всі пакети в своєму каналі прослуховування, навіть якщо вони не призначені для нього.

Мета режиму моніторингу - ін'єкція пакетів. Можна вводити випадкові кадри MAC IEEE 802.11 за допомогою заголовка radiotap і мережевого інтерфейсу WLAN.

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           8812au          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac WLAN Adapter
  (monitor mode enabled)
root@kali:~# airmon-ng stop wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           8812au          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac WLAN Adapter
 (monitor mode disabled)
```

Рис. 1. Результат виконання команд зміни режиму роботи адаптера

Для інтерфейсів карт працює наступний спосіб: airmon-ng start wlan0, де замість wlan0 потрібно вказувати ім'я інтерфейсу.

Включаємо для неї режим моніторингу через 3 послідовні команди: ifconfig wlan0mon down, iwconfig wlan0mon mode monitor, ifconfig wlan0mon up.

На монітор будуть виведені доступні wi-fi мережі. Збір та аналіз пакетів Команда airodump-ng використовується для захоплення бездротових пакетів: airodump-ng wlan0mon. Вона захоплює фрейми 802.11 для подальшого використання їх в aircrack-ng. Після захоплення і аналізу пакетів доступна важлива інформація, така як MAC-адреса, номер каналу і розширений ідентифікатор набору послуг (ESSID) точки доступу.

Базова ідентифікація набору послуг (BSSID) – це MAC-адреса ТД, а STATION показує MAC-адреси бездротових пристроїв підключених до точки доступу (ТД).

Далі необхідно вибрати жертву і реалізувати атаку деавтентифікації. Наприклад, використаємо тестову ТД з прихованим ім'ям і MAC-адресою 34:CE:00:5D:03:7A.

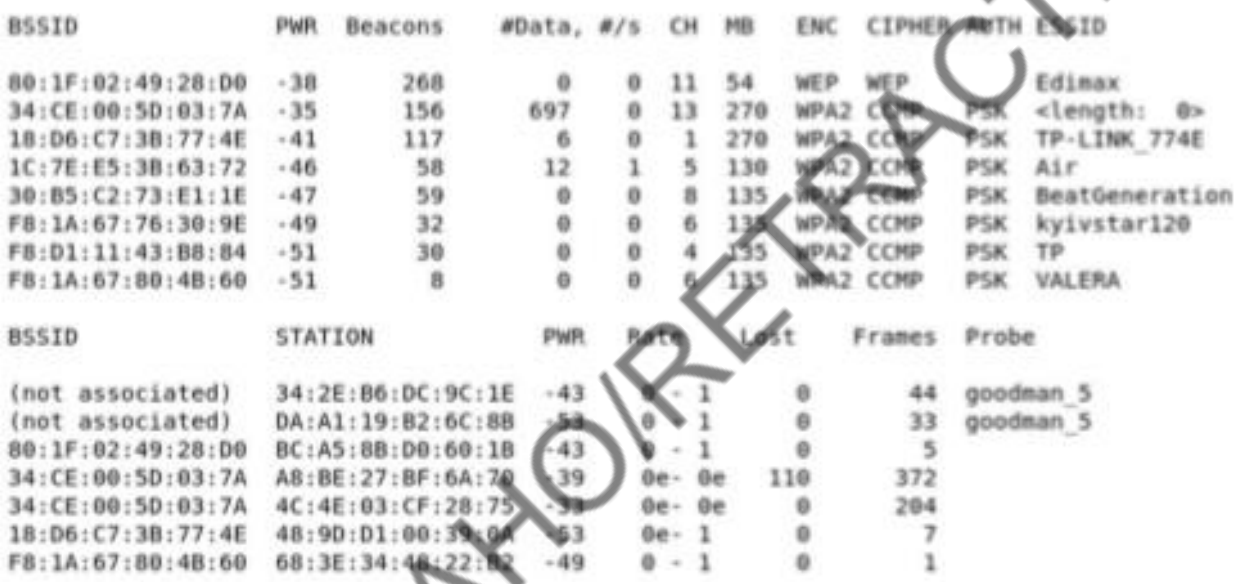

Рис. 2. Результат виконання команди airodump-ng

Для виконання ін’єкції кадрів успішної атаки необхідно перевести мережну карту на потрібний канал і для відправки пакетів deauth використовувати команду aireplay-ng із зазначенням MAC-адреси ТД і MAC-адреси клієнта.

Встановити канал можна командою iwconfig wlan0 channel n, де замість n потрібно підставити номер каналу: iwconfig wlan0 channel 13 та виконання ін’єкції кадрів командою: aireplay-ng -0 0 -a 34: CE:00:5D:03:7A -c 4C:4E:03:CF:28:75 wlan0, де - «-0» відправляє пакет деавтентифікації, «0» кількість пакетів (значення 0 - переривання вручну), «-a» MAC-адреса точки доступу та «-c» MAC-адреса клієнта, якого необхідно відключити від ТД.

Замість BSSID можна вказувати ім'я ESSID. Робиться це з опцією «-e». Кадри deauth надходили на ТД протягом 30 сек. На час атаки клієнт був повністю відключений від ТД, що унеможливило будь-яку передачу даних.

Якщо все зроблено правильно, то в результаті отримуємо приблизно наступне.

2. Використання вейвлет-перетворення для виявлення атаки

Техніка вейвлет-аналізу широко використовується в системах виявлення атак, завдяки частотно-часовій властивості, яка дозволяє розкладати сигнал на кілька частотних компонент. Вже досить багато робіт було опубліковано на цю тему і багато систем впроваджено на практиці, деякі з них будуть розглянуті в цій роботі[11-13].

Рис. 3. Результат виконання команди aireplay-ng

Зазвичай розрізняють дискретне вейвлет-перетворення (ДВП) і безперервне вейвлет-перетворення (БВП). БВП – це реалізація вейвлет-перетворення з використанням довільних масштабів і практично довільних вейвлетів, тоді як ДВП використовує вейвлети ортогонального типу і масштабування за ступенем двійки. В першому випадку можливе більш детальне вивчення поведінки трафіку, тоді як у другому досягається більш швидке здійснення перетворення[10].

В [11] використовуються чотири різних сімейства вейвлетів. По аналізу різних аномалій Neptune (NP), Mailbomb (MB), Smurf (SM), Port-scan (PS) і Stealth-scan (SS) за допомогою різних вейвлетів. Наведені графіки на рис. 4 є середні процентні відхилення: вейвлет на аномалію. Для оцінки ефективності різних функцій вейвлетів для виявлення різних типів аномалій використовувалося дві метрики, а саме відсоткове відхилення та ентропія.

Демонстровано різні характеристики довжин фільтрів. Неоднорідні характеристики відображаються для одного вейвлета, але з різною довжиною. У разі кращої роботи COIF збільшили довжину фільтра з розміром вікна, приблизно до 60 зразків, щоб побачити ефект. Як зазначається на наступних графіках, COIF.21 перевершував COIF.41 і COIF.61 по локалізації за часом і низькими середніми значеннями відхилень. Подібні ознаки спостерігаються і для інших фільтрів. Як видно на рис. 4 - a, COIF.21 (вейвлет Coiflet, довжина 21), з низькими середніми значеннями відхилення (дисперсії), показує кращі характеристики для всіх аномалій. Вейвлети Daubechies на рис. 4 - b демонструють погані характеристики. Вейвлети з великою довжиною на рис. 4 - d досягають низьких середніх значень відхилення, вони не виявляють доброї локалізації в часі, тому не вважаються придатними для цих аналізів.

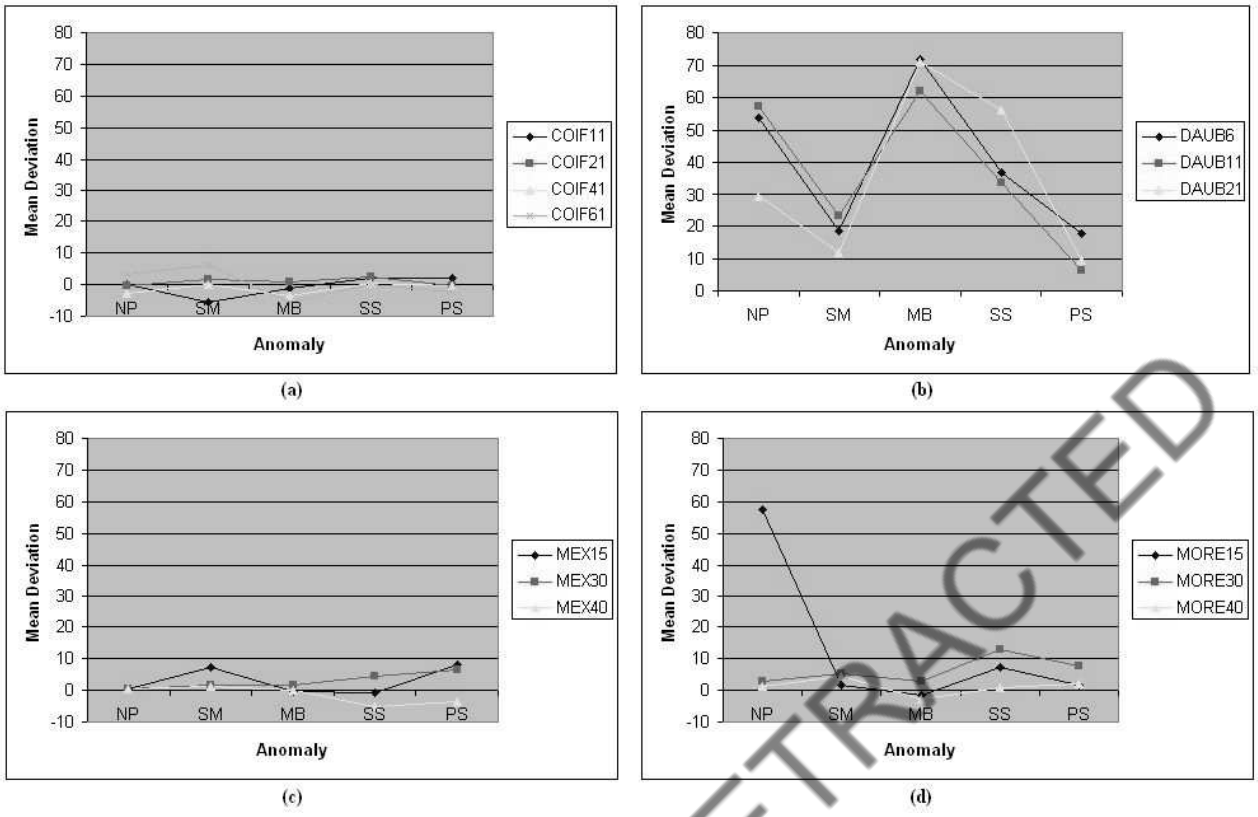

Рис. 4. Середнє відхилення на різних аномаліях для (a) вейвлетів Coiflet, (b) вейвлетів Daubechies, (c) Mexican hat вейвлетів та (d) вейвлетів Morlet.

Порівнюючи коефіцієнти і значення, вейвлети MORE (Morlet) і DAUB (Daubechies) працюють погано. З розглянутих вейвлетів залишилися COIF (Coiflet) і MEX (Mexican hat), бо вони демонструють кращі характеристики. З експериментальних результатів можливо ефективно стверджувати, що для вейвлетів COIF і MEX - 50% або більше відхилення частотних компонентів свідчать про аномалії при аналізі розміром вікна 60 зразків. Зміна довжини вікон і довжини фільтра, може привести до зміни цих порогових значень.

Автоматичне виявлення аномалій в мережевому трафіку є важливим і складним завданням. В [12] демонстровано, що для створення системи вейвлет-аналізу з моніторингу мережевого трафіку доцільно використовувати вейвлет Хаара $\psi_{m,k}(t)$, масштабуючу функцію $\phi_{m,k}(t)$, і алгоритм швидкого вейвлет-аналізу (алгоритм Малла) для отримання найкращого результату в порівнянні IDS(Intrusion Detection System) Snort і StopAttack з створеною на основі використання вейвлет–перетворення програми.

Оцінка ефективності прототипу автоматичної системи виявлення вторгнень проведена на експериментальній ділянці телекомунікаційної мережі системи електронного документообігу і управління взаємодією. Результати експеримент представлені на рис. 5.

У порівнянні з відомими IDS, запропоноване рішення аналізатора аномальності (АА) приймає більш високі характеристики: по швидкодії на 10–12%, по ймовірності пропуску атаки – на 12–22%, при допустимому рівні ймовірності помилкової тривоги 5% і з вірогідністю виявлення 78– 88%.

Розподілена атака відмови в обслуговуванні (DDoS) є однією з головних загроз, оскільки вона прямо загрожує стабільності Інтернету. В [13] представлений систематичний метод виявлення атак DDoS на основі технології ВП. Виявлення атаки може бути виконано за допомогою ідентифікації ненормальної поведінки трафіку. Характеристика мережевого трафіку з моделюванням поведінки може бути кращим методом для виявлення атак. Оскільки масштаби часу можуть бути природним чином представлені вейвлетами, а уявлення вейвлетів також відповідає властивостям бурхливого мережевого трафіку, то для

аналізу трафіку застосовується аналіз масштабування на основі вейвлетів. ВП здатне фіксувати складну часову кореляцію в різних часових масштабах з дуже низькою обчислювальною складністю.

Тип втор-жения	IDS	Ср. время обнар, с	Вер. обнар., $(1-p_{па})$	Оцен-ка точн., $\varepsilon_{рпа}$
Ска-нер пор-	Snort	4,11	0,86	0,04
	StopAttak	3,86	0,84	0,0376
	AA	3,8	0,94	0,028
DOS - атаки	Snort	2,08	0,72	0,0724
	StopAttak	1,22	0,79	0,0674
	AA	0,98	0,84	0,05
Атаки на сервер	Snort	2,78	0,66	0,023
	StopAttak	2,46	0,7	0,046
	AA	2,28	0,84	0,049
spam	Snort	–	–	–
	StopAttak	3,6	0,8	0,0430
	AA	3,15	0,86	0,0469

Рис. 5. Результати порівняльної характеристики IDS

Було використано розподіл енергії на основі ДВП для виявлення трафіку DDoS-атак. Розподіл енергії в часі буде мати обмежені варіації, якщо трафік буде зберігати свою поведінку в часі. У той час як введення аномального трафіку в мережу призведе до значного відхилення розподілу енергії за короткий проміжок часу. Експериментальні результати з інтернет-трафіком показують, що дисперсія розподілу енергії помітно змінюється, викликаючи стрибок дисперсії, коли поведінка трафіку впливає на DDoS-атаку. Цей стрибок дисперсії розподілу енергії може бути зафіксований на ранній стадії атаки, набагато випереджаючи накопичення перевантаження, що робить його ефективним до виявлення атаки.

Як перший крок аналізу, схожість трафіку витягується шляхом оцінки параметра Херста. Модельований трафік також демонструє досить високу самоподібність (всі випадки атаки давали значення параметрів Херста в межах 70-80%). Потім приймається метод для обчислення зміни розподілу енергії різних часових послідовностей. З порогом 0,01 схема змогла зафіксувати всі випадки нападу. Точки знаходження збігаються з часом запуску атаки, на рис. 6.

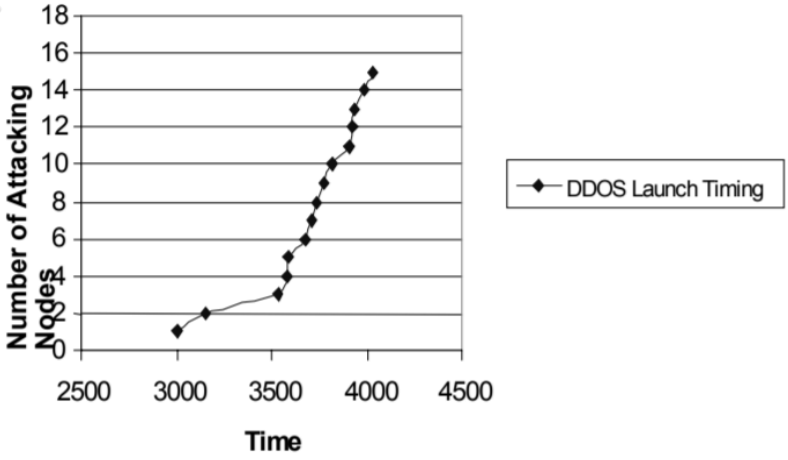

Рис. 6. Час запуску DDoS атаки

3. Експериментальний результат

Для початку аналізу трафіку за обраною технологією треба застосувати вейвлет-перетворення(ВП) і обрати ефективні інструменти вейвлет-аналізу[14]. ВП є поданням сигналу у вигляді узагальненого ряду чи інтегралу Фур'є по системі базисних функцій, які сконструйовані з материнського (вихідного) вейвлета за рахунок операцій зсуву у часі та змінами часового масштабу. Використання вейвлет-спектру дозволить визначити час початку змін частоти сигналу[15].

3.1 Вибір вейвлет–базису

ВП пропонує для обробки даних великий набір інструментів [16], які допомагають розділити вихідний сигнал на складові і побачити його структуру на різних масштабах. Вибір вейвлет-базису є важливою проблемою перед початком процедури виявлення. Але не існує універсального методу, який запропонує вибір вейвлет-базису. Вибір вейвлета залежить від вихідного сигналу [17].

Вейвлет Хаара має компактний носій і забезпечує реконструкцію сигналу та функції. Кожна функція суворо локалізована у фізичному просторі (у часі), але характеризується повільно спадаючим спектром частот. Тобто просторові (часові) та частотні характеристики не можна одночасно вимірювати з довільно високою точністю. Перевагами базису Хаара є те, що для нього розроблені швидкі алгоритми виконання ДВП[18]. Точність вимірювання просторових характеристик (1) Δx та частотних характеристик Δω обмежена відношенням Гейзенберга:

$$\Delta x \Delta \omega \geq \frac{1}{2} \tag{1}$$

3.2 Використання дискретного вейвлет–пакетного перетворення

При безперервній зміні параметрів для розрахунку вейвлет - спектра необхідні великі обчислювальні витрати. Більшість функцій вейвлетів надлишкові. Необхідна дискретизація цих параметрів при збереженні можливості відновлення сигналу з його перетворення [19].

Сутність операцій алгоритму Малла полягає в наступному. Подання сигналу у вигляді сукупності послідовних наближень апроксимуючої і деталізують складових до яких використовується набор фільтрів – низькочастотний і високочастотний. Спочатку сигнал пропускається через низькочастотний фільтр, в результаті чого виходять коефіцієнти апроксимації, які характеризують глобальний тренд досліджуваного ряду. Вихідна послідовність також пропускається через високочастотний фільтр, при цьому на виході виходять коефіцієнти деталізації, що характеризують локальні особливості ряду даних. Для збільшення частотного дозволу можливе проведення повторного розкладання для коефіцієнтів апроксимації попереднього рівня.

При розгляді дискретного вейвлет – пакетного перетворення(ДВПП) за алгоритмом Малла [20] на кожному кроці відбувається «розщеплення» сигналу на високочастотні і низькочастотні складові та «відсікання» високочастотної складової. Причина такого підходу полягає в неявному припущенні, що низькочастотна область містить більше інформації про вихідний сигнал, ніж високочастотна область. Розпізнавання за вейвлет-коефіцієнтами, яких у декілька разів менше, ніж дискрет сигналу, дозволить зменшити обчислювальні витрати[21].

Застосування ДВПП надає ширшу частину діапазону частот, ніж ДВП. З безлічі можливих базисів вейвлет-розкладання на всіх рівнях деталізації експериментально з урахуванням часових обмежень вибираються ті, на яких аномальний стан трафіку проявляється найбільш чітко.

В якості критерію вибору оптимального базису запропоновано використовувати критерій мінімуму ентропії, що характеризує рівень усереднення і визначає кількість

істотних коефіцієнтів моделі трафіку. Критерій, за яким проводиться виявлення аномалій, являє собою відношення дисперсій і середнього коефіцієнтів ДВПП. Адаптація вибору рівня розкладання полягає в наступному. Якщо на якомусь рівні пакетного перетворення є перевищення верхнього порогу, виноситься рішення про наявність аномалії. Якщо ж на цьому рівні відбувається перевищення нижнього порога, значить, в цьому місці можливо має місце бути аномалія і тоді проводиться подальша вейвлет-декомпозиція до наступного рівня, на якому знову проводиться аналіз. Так відбувається до того моменту, поки значення відносин або не перевищить верхній поріг, що буде говорити про аномалії, або перестане перевищувати порог взагалі, що буде говорити про відсутність аномалій.

На рис. 10 зображені графіки вихідного трафіку (справа вгорі), оптимальне дерево розкладання (зліва вгорі) і відновлена випадкова складова трафіку по одному вузлу (6.1) (зліва внизу). Аномалія в даному випадку є результат атаки SYN-Flood. Також показано, що на відновленій випадкової складової трафіку піки збігаються на часовій осі з аномаліями на вихідному трафіку, тобто аномалії добре локалізуються за допомогою зворотного ДВПП при використанні вибіркових вузлів оптимального дерева розкладання.

Для проведення експеременту було використано головне меню ToolBox Wavelet - wavemenu з обраною опцією – wavelet-packet 1-D.

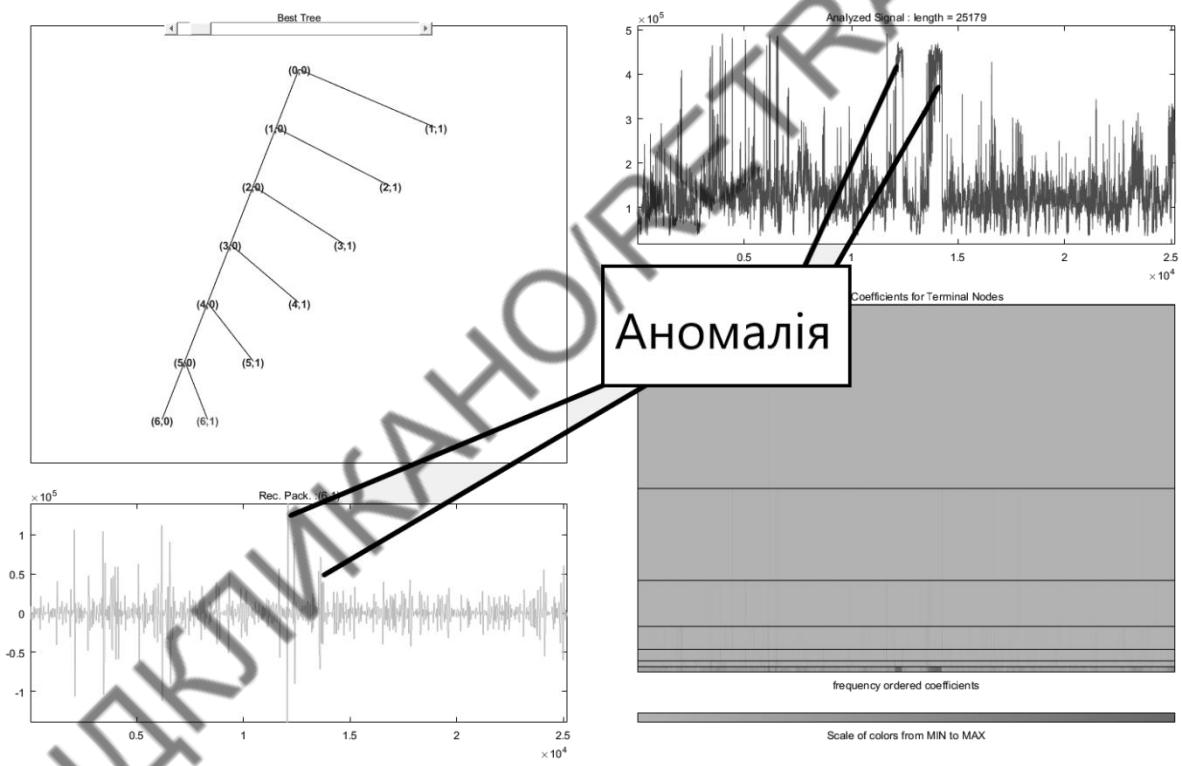

Рис. 7. Результати вейвлет-пакетного розкладання трафіку по базисним функція Хаара і відновлення по високочастотним вузлів кращого дерева розкладання: (6,1)

Висновки та рекомендації. За результатами дослідження можна зробити висновок про те, що для бездротових клієнтів в мережі стандарту 802.11 існує вразливість, згідно з якою зловмисник може реалізувати DoS-атаку - нескінченно відправляти пакети деавтентифікації, що дозволяє відключити клієнтів на тривалий час від точок доступу, до яких вони підключені. Під час виконання роботи було розроблено власну методику виявлення аномалій і мережевих атак на основі інтеграції вейвлет-пакетної моделі мережевого трафіку в інтерактивному середовищі розробки Matlab, а саме було визначено ряд параметрів, які враховуються при здійсненні ВП.

Розглядаючи особливості цієї роботи можна зробити наступні рекомендації:

аномалії мережевого трафіку можна розділити на два великі класи – короткочасні і довготривалі.

застосування вейвлет-функції Хаара для підвищення характеристики правильного виявлення у системах виявлення на основі ВП;

при зміні довжини фільтра вейвлетів можливе спостереження підвищення ефективності виявлення.

проведено аналіз ефективності алгоритмів ВП, що загалом становить 70-94% правильного виявлення аномалії;

при використанні ВП стає помітен стрибок дисперсії розподілу енергії який може бути зафіксований на ранній стадії атаки, набагато випереджаючи накопичення перевантаження, що робить його ефективним для виявленням атаки;

перспективним є метод з виявлення аномалії мережевого трафіку за допомогою ентропії [22];

алгоритм Малла дає можливість аналізу частотно-часового подання сигналу по низькочастотних і високочастотних компонентів, що забезпечує можливість локалізації аномалій сигналу різних видів;

використання ДВПП, що значно знижує обчислювальні витрати у розкладанні компонентів ВП.

Перелік посилань

1. 1. Compton, S. and Hornat, C., "802.11 denial of service attacks and mitigation", SANS Institute InfoSec Reading Room, 2007, pp.14-18.

2. Tverdohleb J.V. Processing of ECG signals based on wavelet transformation / J.V. Tverdohleb, V.I. Dubrovin // International journal of advanced science and technology. – 2011. – Vol. 30. – P. 73-81.

3. J. Tverdohleb Non-pharmacological correction methods of central nervous system disturbances / V. Dubrovin, M. Zakharova, A. Rashavchenko, J. Tverdohleb // Proceedings of Information Technologies In Innovation On Business Conference. – Kharkiv: KhNURE, 2015. – P. 43-46.

4. J. Tverdohleb Wavelet technologies of non-stationary signals analysis / J. Tverdohleb, V. Dubrovin, M. Zakharova // 1-th IEEE International Conference on Data Stream Mining & Processing. – Ukraine, Lviv: LPNU, 2016. – P. 75-79.

5. M. Vipin and S. Srikanth, "Analysis of open source drivers for IEEE 802.11 WLANs," 2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC), Chennai, 2010, pp. 1-5.

6. Р. Корольков, С. Куцак Особливості реалізації атаки деавтентифікації в мережах стандарту 802.11 // Ukrainian Information Security Research Journal, —2019. — Т. 21. — № 3. — С. 175-181.

7. H. Peng, "WIFI network information security analysis research", Proceedings of 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). Yichang, pp. 2243-2245, 2012.

8. D. Joshi, Dr. Ved Vyas Dwivedi, K. Pattani, "De-Authentication attack on wireless network 802.11i using Kali Linux" IRJET, Volume 04, Issue 01, pp. 1666-1669, Jan 2017.

9. R. Cheema, D. Bansal, Dr. Sanjeev Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", International Journal of Computer Applications, Volume 23, No.7, pp. 7-15, June 2011.

10. Shwan Dyllon and Perry Xiao (October 3rd 2018). Wavelet Transform for Educational Network Data Traffic Analysis, Wavelet Theory and Its Applications, Sudhakar Radhakrishnan, - 2018. – 268p.

11. C. Huang, S. Thareja and Y. Shin, "Wavelet-based Real Time Detection of Network Traffic Anomalies," 2006 Securecomm and Workshops, Baltimore, MD, pp. 1-7.

12. Соловьев, Н.А. Обнаружение вторжений на основе вейвлет–анализа сетевого трафика / Н.А. Соловьев, Н.А. Тишина, И.Г.Дворовой // Вестник УГАТУ / научно практический журнал. – Уфа. – 2010. – Т .14, №5(40). – С. 188 – 194.

13. Li, L., Lee, G. DDoS Attack Detection and Wavelets. Telecommun Syst 28, 2005, pp. 435–451.

14. Твердохліб Ю. В. Методи та інформаційна технологія комплексного оцінювання параметрів вейвлет-перетворення нестаціонарних сигналів [Текст]: автореф. дис. ... канд. тех. наук: 05.13.06 / Твердохліб Юлія Володимирівна; Харків. нац. екон. ун-т ім. Семена Кузнеця. – Харків, 2018. – 20 с.

15. Аносов, М.М. Проценко, О.Л. Дубинко, М.Я. Павлунько Застосування вейвлет-перетворення для аналізу цифрових сигналів//Сучасний захист інформації. - №1(33), - 2018, - рр.38-42.

16. Пат. 90102 Україна, МПК6 G01R 23/16. Спосіб визначення оптимального вейвлету для аналізу сигналів на основі дослідження його амплітудно-частотної характеристики [Текст] / В.І. Дубровін, Ю.В.

Твердохліб; заявник и патентовласник: Запорізький національний технічний університет. - заявл. 20.12.13; опубл. 12.05.14, Бюл. №9., 3с.

17. Dubrovin V.I. R-peaks detection using wavelet technology / V.I. Dubrovin, J.V. Tverdohleb, V.V. Kharchenko// Радиоэлектроника, информатика, управление. – 2013. – №2 (29). – P. 126-129.

18. Проценко, М.М. Павлунько, М.Я. Мороз, Д.П. Бржевська З.М. Методика фільтрації цифрових сигналів з використанням швидкого вейвлет-перетворення //Сучасний захист інформації. - №1(37), - pp. 64-69, – 2019.

19. Шелухин, О. И. Обнаружение DOS и DDOS-атак методом дискретного вейвлет-анализа / О. И. Шелухин, А. В. Гармашев // T-Comm-Телекоммуникации и Транспорт. — 2011. — № 1. — С. 44-46.

20. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) // Научно – техническое издательство Горячая линия – Телеком. 2016. —211с.

21. Проценко, М.М. Куртсеітов, Т.Л. Павлунько, М.Я. Бржевська, З.М. Застосування пакетного вейвлет-перетворення для обробки радіотехнічних сигналів//Сучасний захист інформації. – №3(35). – 2018, – pp.11-15.

22. Дубровин В.И. Исследование изменений энтропии и энергии на этапах декомпозиции сигнала / Дубровин В.И., Твердохлеб Ю.В. // Радиоэлектроника, информатика, управление. – 2013. – №2 (29). – С. 54-58.

Надійшла: 30.03.2020 Рецензент: д.т.н., професор Савченко В.А.