УДК 004.65:620.92

Б. В. ПЕТРИК, Г.В. НЕЛАСА, В. І. ДУБРОВІН
Національний університет «Запорізька Політехніка»

АНАЛІЗ ЧАСОВИХ ПОСЛІДОВНИХ ПОТОКІВ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ НА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

В даний час для вивчення властивостей в мережевих системах і їх процесів широко застосовується підходи, засновані на аналізі їх вихідних сигналів. Тому аналіз систем і процесів, особливо при експериментальних дослідженнях, часто реалізується за допомогою обробки реєстрованих сигналів. Майже в кожній предметній області існують явища, які необхідно вивчати в їх динаміці, а сукупність реєстрованих сигналів подібного роду за певний період часу і є часові послідовності потоків даних. Для аналізу часових послідовностей, які є стаціонарними або нестаціонарними випадковими процесами, використовують традиційні методи статистичного аналізу випадкових величин і функцій. Найбільш поширеними з них є кореляційний і спектральний аналізи, згладжування і фільтрація даних, моделі авторегресії і прогнозування. Поряд з традиційними методами, в останні роки набувають поширення способи обробки сигналів, засновані на вейвлет-перетворенні. Особливість цієї технології в тому, що вона дозволяє розкрити особливості локальної структури складного сигналу і виявити різні його властивості, невидимі в режимі реального часу. В області вейвлет-перетворення виділяється додаткова інформація за допомогою подання до частотно-часового зображення сигналу, недоступного в початковому вигляді. На сьогоднішній момент часу посилюються вимоги до якіснішого виявлення внутрішніх закономірностей в поведінці часових послідовностей і прогнозом періодів стійкості досліджуваних процесів. Тому виникає необхідність в розробці нових і модифікації існуючих алгоритмів аналізу часових послідовностей в мережевих системах. У даній роботі досліджено застосування вейвлет-перетворення для виявлення вторгнень в комп'ютерні мережі. Пропонується аналіз останніх досліджень по даній задачі, де розглянуті вже існуючі алгоритми та методи виявлення атак за допомогою вейвлет-перетворення. Важливим пунктом у цій роботі є обґрунтування застосування вейвлет–функції та алгоритму вейвлет-перетворення для аналізу часових послідовних потоків даних мережевого трафіку. З використанням вейвлет-функції пропонується усунення шуму з мережевого трафіку та з використанням пакетного вейвлет-перетворення для аналізу мережевого трафіку і отримання інформації про можливі атаки. Використання вейвлет-функції має важливий характер, бо вибір оптимального вейвлет-базису дозволить підняти ймовірність виявлення як на початковому етапі, так і при реконструкції сигналу.

Ключові слова: вейвлет-перетворення, шумозниження, мережевий трафік, мережева атака, вейвлет Хаара, алгоритм Малла.

Б. В. ПЕТРИК, А. В. НЕЛАСАЯ, В. И. ДУБРОВИН
Национальный университет «Запорожская Политехника»

АНАЛИЗ ВРЕМЕННЫХ ПОСЛЕДОВАТЕЛЬНЫХ ПОТОКОВ ДАННЫХ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

В настоящее время для изучения свойств в сетевых системах и их процессов широко применяется подходы, основанные на анализе их выходных сигналов. Поэтому анализ систем и процессов, особенно при экспериментальных исследованиях, часто реализуется с помощью обработки регистрируемых сигналов. Почти в каждой

10.32782/2618-0340/2020.1-3.17

предметной области существуют явления, которые необходимо изучать в их динамике, а совокупность регистрируемых сигналов подобного рода за определенный период времени и является временные последовательности потоков данных. Для анализа временных последовательностей, которые являются стационарными или нестационарными случайными процессами, используют традиционные методы статистического анализа случайных величин и функций. Наиболее распространенными из них являются корреляционный и спектральный анализы, сглаживание и фильтрация данных, модели авторегрессии и прогнозирования. Наряду с традиционными методами, в последние годы получают распространение способы обработки сигналов, основанные на вейвлет-преобразовании. Особенность этой технологии в том, что она позволяет раскрыть особенности локальной структуры сложного сигнала и выявить различные его свойства, невидимые в режиме реального времени. В области вейвлет-преобразования выделяется дополнительная информация с помощью представления в частотно-временном изображении сигнала, недоступного в первоначальном виде. На сегодняшний момент времени усиливаются требования к качественному выявлению внутренних закономерностей в поведении временных последовательностей и прогнозу периодов устойчивости исследуемых процессов. Поэтому возникает необходимость в разработке новых и модификации существующих алгоритмов анализа временных последовательностей в сетевых системах. В данной работе исследовано применение вейвлет-преобразования для обнаружения вторжений в компьютерные сети. Предлагается анализ последних исследований по данной задаче, где рассмотрены уже существующие алгоритмы и методы обнаружения атак с помощью вейвлет-преобразования. Важным пунктом в этой работе является обоснование применения вейвлет-функции и алгоритма вейвлет-преобразования для анализа временных последовательных потоков данных сетевого трафика. С использованием вейвлет-функции предлагается устранения шума с сетевого трафика и с использованием пакетного вейвлет-преобразования для анализа сетевого трафика и получения информации о возможных атаках. Использование вейвлет-функции имеет важный характер, потому что выбор оптимального вейвлет-базиса позволит поднять вероятность обнаружения как на начальном этапе, так и при реконструкции сигнала.

Ключевые слова: вейвлет-преобразования, шумопонижения, сетевой трафик, сетевая атака, вейвлет Хаара, алгоритм Малла.

B. V. PETRIK, H. V. NELASA, V. I. DUBROVIN
National University 'Zaporizhzhia Polytechnic'

ANALYSIS OF TIME SERIAL FLOWS OF NETWORK TRAFFIC DATA BASED ON A WAVELET TRANSFORM

Currently, approaches based on the analysis of their output signals are widely used to study the properties in network systems and their processes. Therefore, the analysis of systems and processes, especially in experimental studies, is often implemented through the processing of recorded signals. In almost every subject area there are phenomena that need to be studied in their dynamics, and the set of registered signals of this kind for a certain period of time and there are time sequences of data flows. For the analysis of time sequences, which are stationary or non-stationary random processes, traditional methods of statistical analysis of random variables and functions are used. The most common of these are correlation and spectral analysis, data smoothing and filtering, autoregression models and prediction. Along with traditional methods, wavelet transform methods based on wavelet

10.32782/2618-0340/2020.1-3.17

transform have become widespread in recent years. The peculiarity of this technology is that it allows you to reveal the features of the local structure of a complex signal and detect its various properties, invisible in real time. In the wavelet transform area, additional information is selected by presenting to the frequency-time image a signal that is not available in its original form. At present, the requirements for better detection of internal patterns in the behavior of time sequences and the forecast of periods of stability of the studied processes are increasing. Therefore, there is a need to develop new and modify existing algorithms for analyzing time sequences in network systems. In this work, we investigate the use of wavelet transform to detect intrusions into computer networks. The analysis of the last researches on the given problem where the already existing algorithms and methods of detection of attacks by means of wavelet transform are considered is offered. An important point in this paper is the substantiation of the application of the wavelet function and the wavelet transform algorithm for the analysis of time sequential data flows of network traffic. Using the wavelet function, it is proposed to eliminate noise from network traffic and using packet wavelet conversion to analyze network traffic and obtain information about possible attacks. The use of the wavelet function is important, because the choice of the optimal wavelet basis will increase the probability of detection both at the initial stage and during the reconstruction of the signal.

Keywords: wavelet-transform, de–noise suppressor, network traffic, network attack, wavelet Haar, Mallat algorithm.

Постановка проблеми

Системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи вже давно застосовуються як один з необхідних рубіжів оборони інформаційних систем і використовуються для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпеку комп'ютерної системи. Небезпечним процесом в інтернет–мережі є мережева атака [1]. Аналіз даних мережевої безпеки дуже важливий для виявлення мережевих атак. У даний час існує багато методів виявлення мережевих атак, але найефективніші вимагають або відомих параметрів атаки, або більшої обчислювальної потужності. Тобто швидкий і точний пошук по змістовним запитам вкрай важливий, щоб такі численні потоки даних були захищені.

Аналіз останніх досліджень і публікацій

Аналіз існуючих методів розв'язання задачі виявлення вторгнень в комп'ютерні мережі показує, що техніка вейвлет-перетворення широко використовується в системах виявлення атак, завдяки властивому їй частотно-часової властивості, яка дозволяє розкладати сигнал на кілька частотних компонентів. Вже досить багато робіт було опубліковано на цю тему, і багато систем впроваджено на практиці, деякі з них будуть розглянуті в цій роботі.

В роботі [2, С. 147–151] автори в якості вихідних даних використовували агреговані за п'ятихвилинні інтервали, середні значення наступних величин: кількість байт в секунду, кількість пакетів в секунду, кількість потоків в секунду, величина середнього розміру TCP–пакета. У кожному разі зібрані дані представляли собою дискретну послідовність частотно-часового сигналу, який згідно із запропонованим алгоритмом вейвлет-перетворення був розкладений у вигляді ієрархії декількох шарів. Для кожного з витягнутих сигналів змінна часу була незалежною. Наявність різких амплітуд в кожному з представлених сигналів відповідає певним групам аномалій.

Після збору і аналізу трафіку, автори виділяють чотири типи аномалій в реальній мережі:

10.32782/2618-0340/2020.1-3.17

- проблеми обладнання: відмова обладнання або тимчасова невірна настройка обладнання, відключення;
- атаки: DDoS, зазвичай типу flood;
- перевантаження: на мережі, наприклад збільшення величини вихідного трафіку ftp–сервера внаслідок появи на ньому популярного контенту;
- інші аномалії, які не належать ні до проблем на мережі, ні до атак і перевантажень.

Інструментарій вейвлет-перетворення дозволяє виділяти дані аномалії шляхом поділу трафіку на високочастотні, середньочастотні та низькочастотні компоненти (рис. 1). Ключовою ідеєю в роботі є виділення з даного сигналу x (який являє собою середні 5–хвилинні значення) трьох сигналів наступним чином.

Низькочастотна частина вихідного сигналу отримана реконструкцією всіх низькочастотних вейвлет–коефіцієнтів, починаючи з рівня 9 і вище. Ця частина сигналу повинна захоплювати особливості і аномалії дуже високої тривалості (від декількох днів і більше). Середньочастотна частина сигналу отримана реконструкцією вейвлет-коефіцієнтів частотних рівнів 6, 7 і 8. Отриманий тут сигнал має нульове середнє і призначений для захоплення в основному денних коливань сигналу. Число елементів даних тут близько 3% від вихідного сигналу.

Високочастотна частина складається з невеликих короткострокових змін, які вважаються шумом, що ніяк не допомагає в об'єктивному визначенні аномалій.

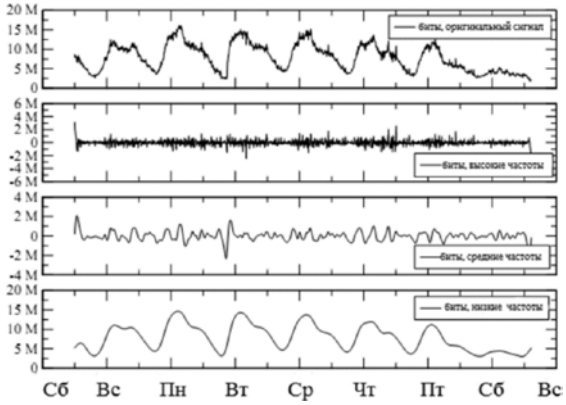

Рис. 1. Вихідний трафік, записаний протягом тижня (вгорі), і його частотні складові.

Після виділення трьох частотних складових сигналу автори обчислюють локальну дисперсію для кожної з цих складових за допомогою ковзного вікна, отримуючи на виході графік зміни дисперсії.

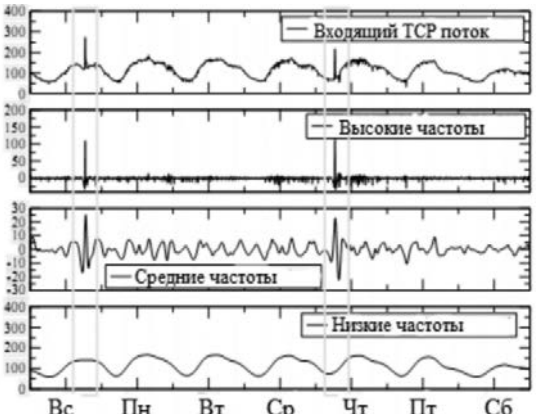

Рис. 2. Вихідний трафік з DOS–атакою(виділена сірими вертикальними смугами) та вейвлет–розкладання за трьома складовими.

10.32782/2618-0340/2020.1-3.17

Далі, застосовуючи пороговий аналіз до цього графіку, по перевищенню порогів приймається рішення про наявність чи відсутність аномалії. Результатом вейвлет-перетворення за методом Барфорду, з'явився важливий висновок про те, що різні типи аномалій можуть бути виявлені на різних, властивих тільки їм, частотних рівнях вейвлет–розкладання. Наприклад, SYN–flood атака, яка представляє собою короткочасну високочастотну аномалію, може бути виявлена тільки на високочастотних і середньочастотних частинах, в той час як на низькочастотній складовій її не видно, що ілюструється на рис. 2. Загалом дослідження показують, що аномалії мережевого трафіку можна розділити на два великі класи – короткочасні і довготривалі.

В роботі [3] показано, що для моніторингу мережевого трафіку доцільно використовувати вейвлет Хаара, і алгоритм Малла для отримання найкращого результату в порівнянні з Snort і StopAttack з створеної 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. 3.

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

Рис. 3. Результати порівняльної характеристики IDS.

У порівнянні з відомими IDS, запропоноване рішення аналізатора аномальність (АА) володіє більш високими характеристиками: по швидкодії на 10–12%, по ймовірності пропуску атаки – на 12–22%, при допустимому рівні ймовірності помилкової тривоги 0,05 і з вірогідністю виявлення 0,78–0,88.

Мета дослідження

Метою даного дослідження є створення методу виявлення мережевих атак з урахуванням особливості методу вейвлет-перетворення. Якість створеного методу, його машинна ефективність залежить від вдало обраних вейвлет-функції та алгоритму використання вейвлет-перетворення.

Викладення основного матеріалу дослідження

Вступ. Вейвлет–перетворення на сьогоднішній день є однією з найбільш перспективних технологій аналізу даних, його інструменти знаходять застосування в самих різних сферах інтелектуальної діяльності. На відміну від перетворення Фур'є, вейвлет–перетворення дозволяє виділяти одночасно як частотну, так і часову компоненти мінливості, тобто дає можливість аналізувати часову мінливість частотного спектра процесу. Оскільки вейвлети мають гарну частотно–часову

10.32782/2618-0340/2020.1-3.17

адаптацію, вони можуть служити зручним інструментом для дослідження частотних характеристик нестаціонарного сигналу [4]. Тобто уявлення мережевого трафіку в різних масштабах. Перевага такого підходу – характерні деталі, які можуть залишатися непоміченими при одному масштабі, легко можуть бути виявлені на іншому.

Також вейвлет– перетворення можливо використовувати для аналізу дискретних даних, у випадках, коли потрібна висока швидкість обробки та аналізу інформації, що актуально для вирішення завдання запобігання мережевих атак.

Вибір вейвлет–функції. На сьогоднішній день існує ціле розмаїття сімейств вейвлет–функцій, кожне з яких має свої переваги для вирішення завдань різних типів. У загальному випадку, зі збільшенням числа коефіцієнтів вейвлета, функції стають більш гладкими, що може полегшити виявлення мережевої атаки.

В даному випадку було обрано вейвлет Хаара бо, його функція має: компактний носій і забезпечення реконструкції сигналу і функції, сувору локалізацію у фізичному просторі (у часі), та характеристику з повільно спадаючим спектром частот [5]. Графічне зображення вейвлета Хаара показано на рис. 4 – а.

Точність вимірювання просторових характеристик (1) Δx та частотних характеристик Δω обмежена відношенням Гейзенберга:

$$\Delta x \Delta \omega \geq \frac{1}{2}. \qquad (1)$$

Розкладання сигналу в системі базисних функцій Хаара має наступну структуру. Перша базова функція – пряма лінія. У разі нормованого базису згортка першої базисної функції з вихідним сигналом буде визначати середнє значення функції. Наступні базисні функції розкладання Хаара є масштабовані за ступенем двійки зсунуті сходинки
(рис. 4 b).

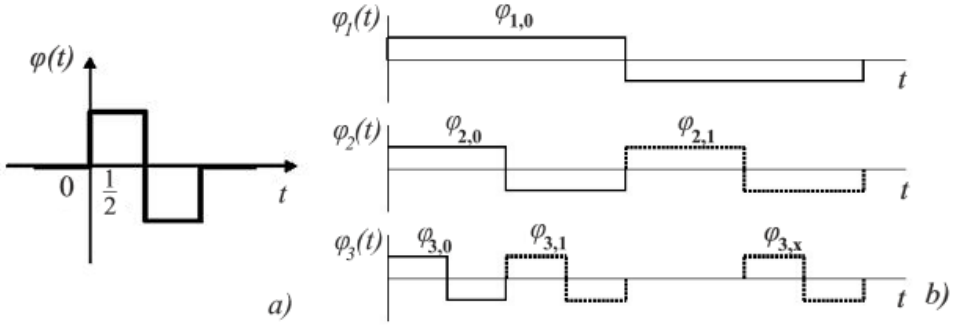

Рис. 4. Зображення вейвлет Хаара (a) та функцій Хаара для різних масштабів згорток (b).

Очищення шуму за допомогою вейвлетів. Шумами прийнято вважати високочастотні компоненти сигналу. Шумозниження є важливим процесом усунення шумів з корисного сигналу з метою підвищення його суб'єктивного якості або для зменшення рівня помилок у каналах передачі і системах зберігання цифрових даних.

Всі пристрої запису, як аналогові, так і цифрові, мають властивості, які роблять їх сприйнятливими до шуму. Часто в лініях зв'язку сигнали піддаються впливу перешкоди «білого шуму», який створює деталізуючи коефіцієнти з високим вмістом шумових компонентів, що мають великі випадкові викиди значень сигналу. При вейвлет–аналізі подібні складові можуть бути видалені з використанням процедури перерахунку коефіцієнтів деталізації, значення яких є меншими в порівнянні зі значенням порога. Процедура усунення шуму [6] має такий алгоритм:

10.32782/2618-0340/2020.1-3.17

1. Декомпозиція. Вибір вейвлета і рівень розкладання, і обчислюється вейвлет-перетворення вихідного сигналу до обраного рівня.
2. М'яка порогова обробка для кожного рівня деталізують коефіцієнтів.
3. Вейвлет-реконструкція, заснована на початкових апроксимуючих коефіцієнтах і модифікованих деталізуючих коефіцієнтах.

Таким чином, можливо встановити шумовий поріг. Ті значення, які перевищують поріг, будуть розглядатися як корисні коефіцієнти сигналу, а ті значення, які менше порога, будуть розглядатися як сигнали шуму, які можна фільтрувати.

На рис. 5 представлений оригінальний(a) і очищений від шуму (b) сигнал в Matlab:

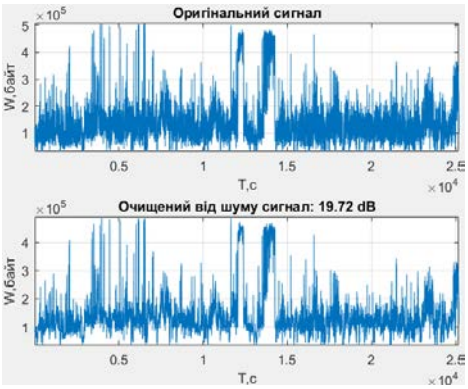

Рис. 5. Зображення оригінального (a) і очищеного від шуму сигналу (b).

Розмір очищеного від шуму сигналу набагато менше, ніж у вихідного сигналу, тому дані будуть займати менше місця і краще підходити для передачі в інтернеті.

Вейвлет-перетворення на основі алгоритму Малла. При безперервній зміні параметрів трафіку для розрахунку вейвлет-спектра необхідні великі обчислювальні витрати. Безліч функцій вейвлетів надлишкові. Необхідна дискретизація цих параметрів при збереженні можливості відновлення сигналу з його перетворення.

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.

Дискретне вейвлет–пакетне перетворення. При розгляді дискретного вейвлет – пакетного перетворення за алгоритмом Малла 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. В результаті виходить «однобоке» дерево (рис. 6).

10.32782/2618-0340/2020.1-3.17

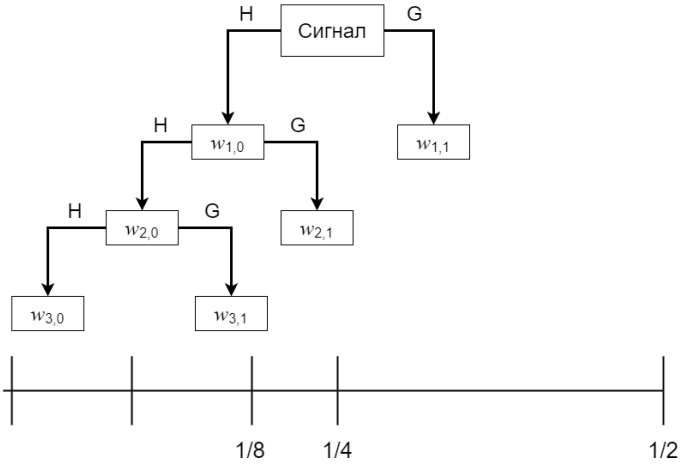

Рис. 6. Логічне уявлення алгоритму Малла.

Таке припущення виправдане для багатьох реальних сигналів, однак для деяких воно не виконується, оскільки вейвлет-аналіз є поведінковим методом [7]. Тобто можна зробити висновок про те, що представлені типи аномальних подій можуть бути ідентифіковані на конкретних, притаманних їм частотах.

Віткам дерева відповідатиме набір підпросторів сигналу з базисами, побудованими, як і для однобокого дерева згідно кратномасштабного аналізу. Функції та фільтри, які породжують ці базиси, називаються вейвлет-пакетами і пакетними фільтрами.

Критерій, за яким проводиться виявлення аномалій, являє собою відношення дисперсії і середнього коефіцієнтів пакетного вейвлет-перетворення. Адаптація вибору рівня розкладання полягає в наступному. Якщо на якомусь рівні пакетного вейвлет-перетворення є перевищення 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 подальші вейвлет-перетворення до наступного рівня, на якому знову проводиться аналіз. Так відбувається до того моменту, поки значення відносин або не перевищить поріг, що буде говорити про аномалії, або перестають перевищувати порога взагалі, що буде говорити про відсутність аномалій.

При проведенні експерименту (рис. 7) маємо вікно з зображення самого трафіку (праворуч — вгорі), оптимальне дерево вейвлет перетворення (зліва–вгорі), також вікна відновленої випадкової складової коефіцієнта деталізації трафіку по вузлу 6.1 (зліва–знизу) і кольоровий спектр – за яким і проводиться аналіз (праворуч-знизу).

Були зроблені наступні висновки – на діапазоні часу [1;1.5 ×10^5 с.] було виявлено дві протяжні аномалії (помічено світло–фіолетовим кольором на кольоровому спектрі). Тобто на відновленій випадковій складовій трафіку (по вузлу 6.1) піки загострення значень збігаються по часовій осі з аномаліями на вихідному трафіку, тобто аномалія(в даному випадку атака SYN–flood) добре локалізуються за допомогою пакетного аналізу вейвлету при використанні вибіркових вузлів оптимального дерева розкладання

Для проведення експерименту було використано середовище Matlab в меню додатку ToolBox Wavelet – wavemenu з обраною опцією – вейвлет–пакетне перетворення.

Таким чином, запропоновану методику на основі інтеграції вейвлет–пакетной моделі мережевого трафіку можна використовувати для виявлення аномальності трафіку і наявності мережевих атак.

10.32782/2618-0340/2020.1-3.17

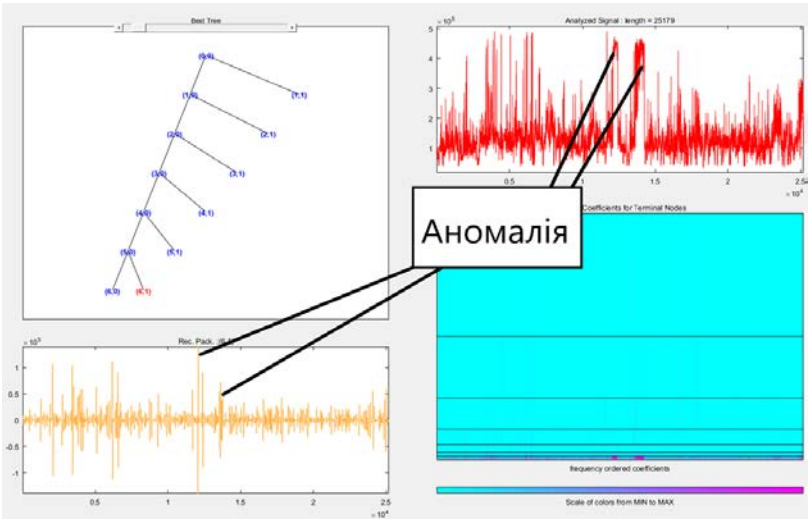

Рис. 7. Результати вейвлет–пакетного перетворення по базисним функціям Хаара і відновлення по деталізуючим вузлам кращого дерева розкладання (6,1).

Висновки

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 вейвлет–перетворення. Тобто вейвлет–функції Хаара використовуються для підвищення характеристики правильного виявлення, а алгоритм Малла дає можливість аналізу частотно–часового подання сигналу по низькочастотних і високочастотних компонентів, що забезпечує можливість локалізації аномалій сигналу різних видів. Також можливе шумозниження сигналу з допомогою вейвлет-перетворення і в результаті зберігання корисних потоків даних мережі для ефективного вилучення аномальних подій.

Список використаної літератури

1. Бєрковський В. В., Безсонов О. С. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему. *Кібернетична безпека*. 2017. №2. С. 57–62.
2. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Москва: Горячая линия – Телеком, 2016. 221 с.
3. Соловьев Н. А. , Тишина Н. А., Дворовой И. Г.Обнаружение вторжений на основе вейвлет–анализа сетевого трафика. *Вестник УГАТУ*. 2010. Т. 14. №5(40). С. 188–194.
4. Tverdohleb J., Dubrovin V., Zakharova M. Wavelet technologies of non–stationary signals analysis. 1–th IEEE International Conference on Data Stream Mining & Processing. (Ukraine, Lviv, 23-27 August, 2016). Lviv: LPNU, 2016. P. 75–79.
5. Твердохліб Ю. В. Методи та інформаційна технологія комплексного оцінювання параметрів вейвлет-перетворення нестаціонарних сигналів : автореф. дис. ... канд. тех. наук: 05.13.06. Харків. нац. екон. ун–т ім. Семена Кузнеця. Харків, 2018. 20 с.
6. SUN Donghong, SHU Zhibiao, LIU Wu, REN Ping, WU Jian–ping. Analysis of Network Security Data Using Wavelet Transforms. *Journal of Algorithms & Computational Technology*. 2003. Vol. 8. №1. P. 59–79.
7. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН*. 2016. №45. С. 211–213.

10.32782/2618-0340/2020.1-3.17

References

1. Bierkovskyi, V. V., & Bezsonov, O. S. (2017). Analiz ta klasyfikatsiia metodiv vyiavlennia vtorhnen v informatsiinu systemu. Kibernetychna bezpeka. **2**, 57–62.
2. Sheluhin, O. I., Sakalema, D. Zh., & Filinova, A. S. (2016). Obnaruzhenie vtorzheniy v kompyuternyie seti (setevyie anomalii). Moskva: Goryachaya liniya – Telekom.
3. Solovev, N. A., Tishina, N. A., & Dvorovoy, I. G. (2010). Obnaruzhenie vtorzheniy na osnove veyvlet–analiza setevogo trafika. *Vestnik UGATU*. **14**, 5(40), 188–194.
4. Tverdohleb, J., Dubrovin, V., & Zakharova, M. Wavelet technologies of non–stationary signals analysis. Proceedings of the *1–th IEEE International Conference on Data Stream Mining & Processing*. (Ukraine, Lviv, 23-27 August, 2016). Lviv: LPNU, pp. 75–79.
5. Tverdokhlib, Yu. V. (2018). Metody ta informatsiina tekhnolohiia kompleksnoho otsiniuvannia parametriv veivlet–peretvorennia nestatsionarnykh syhnaliv: avtoref. dys. ... kand. tekh. nauk: 05.13.06 (PhD Thesis). Kharkiv: Kharkiv. nats. ekon. un–t im. Semena Kuznetsia.
6. SUN, Donghong, SHU, Zhibiao, LIU, Wu, REN, Ping, & WU, Jian–ping. (2003). Analysis of Network Security Data Using Wavelet Transforms. *Journal of Algorithms & Computational Technology*. **8**, 1, 59–79.
7. Branitskiy, A. A., & Kotenko, I. V. (2016). Analiz i klassifikatsiya metodov obnaruzheniya setevyih atak. *Trudy SPIIRAN*. **45**, 211–213.

Дубровін Валерій Іванович – к.т.н., професор, професор кафедри програмних засобів національного університету «Запорізька Політехніка», e–mail: vdubrovin@gmail.com, ORCID: 0000–0002–0848–8202.

Петрик Богдан Вячеславович – студент кафедри програмних засобів національного університету «Запорізька Політехніка», e–mail: dartbogdan32@gmail.com, ORCID: 0000–0002–9528–4610.

Неласа Ганна Вікторівна – к.т.н., доцент, професор кафедри захисту інформації національного університету «Запорізька Політехніка», e–mail: annanelasa@gmail.com, ORCID: 0000–0002–3708–0089.

10.32782/2618-0340/2020.1-3.17