УДК 004.9

Гринченко П.В.[1]

СУЧАСНІ МЕТОДИ ВЕЙВЛЕТ-АНАЛІЗУ

В роботі був запропонований огляд сучасних методів вейвлет-аналізу для моделювання мережевого трафіку, що забезпечує підвищення достовірності прийнятих рішень системами захисту в умовах параметричної невизначеності інформаційних процесів.

Сучасні статистичні методи виявлення порушень у мережі загалом засновані на порівнянні статистичних локальних характеристик потоку пакетів усереднених за відносно невеликий часовий проміжок і їх наступного порівняння із відповідними глобальними характеристиками, що зібрані на тривалому у часі інтервалі.

Аналіз літературних джерел показує, що на сьогоднішній день існує велика кількість алгоритмів виявлення мережевих атак та протидії їм. В даний час серед основних алгоритмів виявлення подібного роду вторгнень можна виділити ряд методів, серед яких:

- алгоритм на основі дискретного вейвлет-перетворення;
- алгоритм Бродського-Дарховського;
- алгоритм на основі суми квадратів вейвлет-коефіцієнтів;
- алгоритм на основі максимуму квадратів вейвлет-коефіцієнтів [1].

За даними дослідження, проведеного аналітичним агентством 42Future на замовлення Qrator Labs, у минулому 2020 році майже чверть найбільших компаній стикалися з DDoS атаками. За останній рік кількість мережевих атак зросла приблизно на 70% від загальної кількості за останні 5 років. Основною метою атак залишається можливість отримання доступу до приватної інформації з подальшим вимаганням шляхом шантажу [2].

Для вирішення задачі виявлення аномалій мережевого трафіку застосовується наведена нижче низка методів.

Алгоритм на основі дискретного вейвлет-перетворення із застосуванням статистичних критеріїв (критерій Фішера і Кохрана). В даному алгоритмі використовується техніка ковзаючих вікон W1 і W2, що дозволяє збільшити надійність виявлення незначних аномалій, метою аналізу яких є викриття мережевої атаки. Перевагами даного алгоритму є здатність ефективного виявлення атаки на кожному з рівнів декомпозиції (при цьому критерій Фішера виявляє атаку найбільш явно). Алгоритм здатний визначити найбільшу кількість атак при початковому рівні розкладання. Водночас із цим, основним недоліком виступає існуюча можливість пропуску аномалії при початку розкладання з більш старших рівнів, на яких підвищується ймовірність виникнення помилкових тривог.

Алгоритм виявлення аномалій Бродського-Дарховського (стандартний режим і режим ковзаючих вікон). При використанні стандартного режиму особливий вплив мають шуми. При виборі алгоритму в режимі ковзаючого

[1] аспірант кафедри САОМ, НУ «Запорізька політехніка»

вікна сукупний вплив перешкод зменшується, і викиди, що характеризують початок і кінець впливу, надаються в більш явному вигляді. Варто зазначити, що для практичної реалізації використовується саме алгоритм в режимі ковзаючого вікна.

Алгоритм, заснований на сумі квадратів вейвлет-коефіцієнтів, що використовує вейвлет Хаара й Добеши задля виявлення аномалій. Алгоритм визначається високою ефективністю, а найбільший ефект від застосування досягається при використанні коефіцієнтів апроксимації для вейвлетів Хаара на верхніх рівнях розкладання. Проте, збільшення розміру вікна аналізу може привести до зростання ймовірності виявлення аномалії, але разом із цим зростає і ймовірність помилкового спрацьовування.

Алгоритм, заснований на максимумі квадратів вейвлет-коефіцієнтів, що заснований на використанні вейвлета Хаара і вейвлета Добеши, чий найбільший ефект відображення аномалій досягається за рахунок використання коефіцієнтів апроксимації із використанням вейвлета Хаара. Алгоритм має меншу ефективність, ніж алгоритм, заснований на сумі квадратів. Найвагомішу роль у виявленні аномалій грають коефіцієнти апроксимації разом із використанням вейвлета Хаара.

Висновки: основними предметами аналізу щодо наведених вище алгоритмів виступають помилки першого й другого родів і кількість правильно виявлених аномалій разом із числом хибних спрацьовувань. Таким чином, за результатами проведеного у роботі аналізу можна зробити висновок про те, що найбільш простими в реалізації й застосуванні є алгоритм Бродського-Дарховського і алгоритм на основі дискретного вейвлет перетворення із застосуванням статистичних критеріїв. Найбільш точним у виявленні аномалій є алгоритм Бродського-Дарховського. Разом із цим при його використанні виявляється менша кількість помилок 1-ого та 2-ого роду, ніж при використанні алгоритму на основі дискретного вейвлет-перетворення із застосуванням статистичних критеріїв. Алгоритм Бродського-Дарховського має найбільшу кількість правильно виявлених аномалій, але у той же час є найбільш ресурсномістким серед наведених.

ПЕРЕЛІК ПОСИЛАНЬ

1. Mehra, Mani Wavelets Theory and Its Applications / Mani Mehra // P.: Springer Singapore, 2018. – 182 p.

2. Debnath, Lokenath Lecture Notes on Wavelet Transforms / Lokenath Debnath // P.: Birkhäuser Basel, 2017. – 220 p.