КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (7), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.7.1730
УДК 004.056.5:004.3

Радівілова Тамара Анатоліївна
к.т.н., доцент, доцент кафедри інфокомунікаційної інженерії ім.В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0001-5975-0269
tamara.radivilova@gmail.com

Кіріченко Людмила Олегівна
д.т.н., професор, професор кафедри прикладної математики
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0002-2780-7993
lyudmila.kirichenko@nure.ua

Тавалбех Максим Хаджарович
аспірант кафедри інфокомунікаційної інженерії ім.В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0002-9629-4183
tavalbeh@icloud.com

Зінченко Петро Петрович
аспірант кафедри прикладної математики
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0002-9119-7720
petro.zinchenko@nure.ua

Булах Віталій Анатолійович
аспірант кафедри прикладної математики
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID: 0000-0002-9177-8787
bulakhvitalii@gmail.com

БАЛАНСУВАННЯ САМОПОДІБНОГО ТРАФІКУ В МЕРЕЖНИХ СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Анотація. У даній роботі розглянута проблема балансування навантаження в системах виявлення вторгнень. Проведено аналіз існуючих проблем балансування навантаження та сучасних методів їх вирішення. Наведено типи систем виявлення вторгнень та їх опис. Представлено опис мережної системи виявлення вторгнень, розташування та функціонування її елементів в комп'ютерній системі. Проведено порівняльний аналіз методів балансування навантаження на основі прийому пакетів та на основі розрахунку часу обслуговування. Також представлено аналіз причин дисбалансу навантаження в елементах системи виявлення вторгнень та наслідків дисбалансу навантаження. Представлено модель мережної системи виявлення вторгнень на основі сигнатурного аналізу пакетів. В даній роботі зазначено мультифрактальні властивості трафіку. На основі проведеного аналізу систем виявлення вторгнень, мультифрактальних властивостей трафіку та проблеми балансування навантаження запропоновано метод балансування, який заснований на роботі елементів системи виявлення вторгнень і аналізі мультифрактальних властивостей вхідного трафіку. Запропонований метод враховує час глибокої перевірки пакетів, що необхідний для порівняння пакета з сигнатурами, який обчислюється на основі розрахунку ступеня мультифрактальності інформаційного потоку. Правила балансування навантаження генеруються за допомогою оціненого середнього часу глибокої перевірки пакетів і параметрів мультифрактальності вхідного навантаження. В даній роботі наведено результати імітаційного моделювання запропонованого методу балансування навантаження в порівнянні зі стандартним методом. Показано, що запропонований в даній роботі метод балансування навантаження забезпечує рівномірний розподіл навантаження на вузлах

системи виявлення вторгнень. Це дозволяє забезпечити високу швидкість і точність визначення вторгнень при якісному балансуванні мультифрактального навантаження.

Ключові слова: балансування навантаження; системи виявлення вторгнень; самоподібний трафік; інформаційні потоки; глибока перевірка пакетів; атаки; дисбаланс навантаження

1. ВСТУП

Виявлення вторгнень (атак) – це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі з метою пошуку ознак можливих інцидентів. Системи виявлення й запобігання вторгнень (СВВ, англ. Intrusion detection system / Intrusion prevention system) є необхідним елементом захисту від мережних атак. Основним призначенням подібних систем є виявлення фактів несанкціонованого доступу в корпоративну мережу і прийняття відповідних заходів протидії. [1-3]

Системи виявлення вторгнень мережі зазвичай розташовуються по периметру мережі або у відносно важливих сегментах мережі, щоб відстежувати різні пакети даних. Вузьким місцем, що впливає на продуктивність мережі, є швидкість обробки мережного пристрою безпеки [4, 5]. СВВ фіксує кожен пакет даних в мережі та вимагає багато часу і системних ресурсів для аналізу і зіставлення пакета даних функції будь-якого типу атаки. Мережні СВВ можуть не виконувати повний аналіз при високих навантаженнях, однак це може привести до того, що деякі атаки не будуть виявлені [6, 7]. Тобто, якщо швидкість виявлення не відповідає швидкості передачі мережних даних, то система виявлення вторгнень мережі не буде враховувати частину пакетів даних, що вплине на коректність і ефективність системи. Також одна з важливих проблем полягає в тому, що більшість мережного трафіку володіє самоподібними (фрактальними) властивостями і має великі викиди даних, що викликає серйозний дисбаланс навантаження при статичних правилах балансування між розподіленими датчиками і може привести до втрати пакетів [8-10]. Отже, розподілена архітектура мережної системи виявлення вторгнень повинна поєднуватися з адекватними динамічними механізмами перерозподілу навантаження. Таким чином, критичною проблемою є розробка методу балансування самоподібного навантаження для підвищення пропускної здатності СВВ.

В даний час існують роботи, які спрямовані на вирішення проблеми балансування навантаження в СВВ. В роботі [11] розглянуто паралельна архітектура СВВ, яка долає обмеження на виявлення вторгнення, розподіляючи навантаження мережного трафіку за масивом вузлів датчиків. Ґрунтуючись на нестандартному обладнанні балансувальника навантажень і економічній ефективності вбудованих датчиків, система використовує нові методи балансування без збереження стану, щоб зменшити обмеження масштабованості. Вона також використовує динамічний зворотний зв'язок від вузлів датчика для адаптації до змін мережного трафіку. В роботі [12, 13] пропонується загальна архітектура для розгортання СВВ в мережі, яка використовує три можливості масштабування: розподіл по шляху для поділу обов'язків, реплікацію трафіку в кластери СВВ і агрегування проміжних результатів для поділу дорогої обробки СВВ. В роботі [14] пропонується метод розподілу самоподібного трафіку між сенсорами СВВ.

Метою даної роботи є модифікація методу балансування навантаження з урахуванням самоподібних властивостей вхідного навантаження для виявлення мережної атаки в СВВ.

ISSN 2663 - 4023

2. ТИПИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Система виявлення вторгнень є комбінацією програмного і апаратного забезпечення для виявлення вторгнень. СВВ можна класифікувати за типом хосту і мережі, що зумовлено різними підходами до категоризації подій безпеки, атак і вторгнень [15, 16].

Система виявлення вторгнень хосту (СВВХ) є прикладом програмної реалізації продукту і встановлюється на один комп'ютер (вузол мережі), отже, детектує атаки, які мають відношення тільки до цього комп'ютера. Як джерело даних зазвичай використовує системні журнали, журнали додатків та інше. Перевага систем такого типу в тому, що вони бачать всю внутрішню структуру комп'ютера і можуть контролювати і перевіряти не тільки зовнішній трафік, а набагато більше об'єктів. Такі системи зазвичай стежать за лог-файлами, намагаються виявити аномалії в потоках подій, зберігають контрольні суми критичних файлів конфігурацій і періодично порівнюють, чи не змінив хтось ці файли.

Система виявлення вторгнень мережі (СВВМ) використовує як джерело дані в мережі. Для визначення ознак нападу в мережі або системі і існування порушень поведінки політик безпеки, інформація збирається в декількох ключових точках в комп'ютерній мережі або комп'ютерній системі і порівнює трафік з наперед заданими патернами (сигнатурами) атак, і, як тільки щось потрапляє під сигнатуру атаки, видається повідомлення про спробу вторгнення. СВВМ також здатні детектувати DoS і деякі інші типи атак, які СВВХ просто не може бачити.

СВВ зазвичай вміє розуміти контент пакетів, заголовки і зміст, прапори і опції, а не тільки порти і IP-адреси. Сучасні СВВ, як правило, складаються з наступних компонент:

- сенсор, який відстежує події в мережі або системі;
- аналізатор подій, виявлених сенсорами;
- компонента прийняття рішення.

У базовому сценарії розподілу трафік рівномірно розподіляється між кожною СВВ в глобальному комплексі локальних СВВ [8]. Це означає, що кожна СВВ мусить отримувати рівний обсяг трафіку. Оскільки сьогоднішні СВВ більш стійкі до стану, ніж попередні покоління, кожна СВВ повинна буде розподілити трафік на основі сеансів, а не окремих пакетів. Таким чином, СВВ може стежити за всім сеансом і бути в курсі будь-яких атак або аномалій. У кожної СВВ повинні бути однакові політики, щоб вони могли зловити одні і ті ж атаки й аномалії. З такими пристроями, як балансувальник навантаження СВВ і комутатор рівня 7, трафік можна відфільтрувати до його відправки в комплекс СВВ [17].

Кращою альтернативою виконання базового рівномірного розподілу трафіку з кожною СВВ є метод, де деякі СВВ отримують тільки певні типи трафіку. Наприклад, якщо комплекс СВВ містив чотири фізичні СВВ, одна з СВВ буде спостерігати тільки HTTP-трафік, одна буде спостерігати тільки за SMTP-трафіком, третя буде спостерігати тільки за трафіком FTP, а четверта СВВ буде спостерігати тільки за DNS і RPC-трафіком. Це дозволить налаштувати кожну СВВ, щоб вони шукали тільки певні типи сигнатур і аномалій атаки [18, 19]. Отже, кожна СВВ налаштована для пошуку тільки певних типів атак. Однак такий метод балансування навантаження не здатний забезпечити задовільний ефект в реальному мережному середовищі. Це обумовлено неоднорідністю мережного трафіку: в реальному мережному середовищі відсоток

трафіку різних додатків не збалансований (HTTP – 47%, UDP – 37%, HTTP video – 9%, VoIP – 1%) [20, 21].

3. ОПИС МЕРЕЖНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Так як архітектура, заснована тільки на одному датчику трафіку, не може бути достатньою для того, щоб протистояти вразливостям в мережах, які характеризуються великим обсягом трафіку, отже, розподілена архітектура з декількома датчиками є найбільш ефективним рішенням для аналізу трафіку і високошвидкісних мереж. Ця розподілена архітектура характеризується набором множини датчиків, які направляють частини мережного трафіку різних датчиків СВВ через деяку політику формування трафіку [20-23].

Кожен датчик СВВ аналізує отриманий трафік на наявність незаконних мережних дій і, за необхідністю, генерує попередження. Основна проблема полягає в тому, що вхідний трафік, який одержує розподілена архітектура СВВ, має самоподібність, яка спричиняє довгострокову залежність, і викиди даних. Тому в роботі пропонується аналіз вхідного трафіку на наявність фрактальних властивостей і динамічний перерозподіл навантаження між датчиками. Для цього можна використовувати балансувальник, який отримує періодичну інформацію про стан датчиків, і на основі деякої політики він здійснює механізм балансування навантаження для переміщення частини мережного трафіку з перевантажених датчиків на менш навантажені [22-25]. Умови навантаження кожного датчика зазвичай оцінюються за допомогою аналізу вхідного трафіку. Однак, в умовах інтенсивного трафіку з несподіваними сплесками надзвичайно складно визначити оптимальну політику прийняття рішень і алгоритм перерозподілу навантаження.

На вхід СВВ надходить трафік (множина пакетів даних) від клієнтів, які розподіляються між датчиками відповідно до політики поділу трафіку за чергами [14, 24]. Кількість пакетів, що надійшли, є загальною кількістю пакетів, що надходять в СВВ протягом заздалегідь визначеного часу. Швидкість надходження пакета є швидкістю, з якою загальні пакети розподіляються між датчиками СВВ. Як правило, СВВ дозволяє розподіляти однакову кількість пакетів для кожного датчику. Іншими словами, спосіб розподілу пакетів при певній швидкості надходження пакета для кожного датчика посилається на спосіб розподілу відповідно до швидкості прибуття пакета. Зазвичай пакети можуть послідовно розподілятися в порядку їх надходження за допомогою циклічного планування, так що пакети можуть бути розподілені за кожним датчиком відповідно до швидкості прибуття.

СВВ мають базу даних відомих вразливостей або відомі шаблони атак (сигнатури) і можуть виявляти ці шаблони в пакетах трафіку, в разі якщо база даних сигнатур включає визначення атаки. Час обслуговування пакета є часом операції, протягом якого проводиться порівняння між сигнатурами і одним або декількома пакетами для виявлення вторгнень. Кожне ядро порівнює кожен або кілька пакетів з однієї або декількома сигнатурами. Чим більше сигнатур присутні для порівняння, тим більше часу необхідно для аналізу. Іншими словами, час обслуговування пакета є пропорційним кількості сигнатур, які повинні бути співставленні з пакетом. Відношення часу обслуговування пакета в одному ядрі до загального часу обслуговування пакета для операції на всіх ядрах називається швидкістю передачі пакетів.

У порівнянні з алгоритмами балансування навантаження на основі прийому пакетів, які зазвичай використовуються, метод визначення навантаження, що підтримує час обслуговування (service time-aware load balancing) збільшує кількість прийнятих і оброблюваних пакетів СВВ, а також зменшує кількість пакетів, які відкидаються [14, 19, 26].

Таким чином, метод визначення навантаження, який підтримує час обслуговування, може швидко виявляти вторгнення навіть при атаці з домінуючим трафіком і великою кількістю сигнатур, що призводить до швидкого збільшення можливостей СВВ. Однак збільшення варіацій пакетів вторгнень і пропускної здатності мережі ускладнює обробку великої кількості трафіку в режимі реального часу. Проблеми для впровадження високошвидкісних СВВ можуть бути типово розбиті на: 1) глибоку перевірку пакетів (Deep Packet Inspection) для високошвидкісного узгодження сигнатур; і 2) спосіб паралельної обробки великої кількості трафіку.

Метод визначення навантаження з підтримкою часу обслуговування використовує час глибокої перевірки пакетів СВВ, в якому зв'язок між трафіком і сигнатурою аналізується з використанням розрахункового часу обслуговування пакета. Час глибокої перевірки пакетів для одного пакета визначається кількістю сигнатур, відповідних пакету. Як правило, у міру збільшення кількості сигнатур, відповідних одиничному пакету, час глибокої перевірки пакетів збільшується, а при зменшенні кількості сигнатур, час глибокої перевірки пакетів зменшується. Однак час глибокої перевірки пакетів залежить не тільки від кількості сигнатур. На час глибокої перевірки пакетів може впливати тип пакета, або стан мережі, або структура мережі.

Відповідно, пристрій балансування навантаження оцінює середній час глибокої перевірки пакетів пакета з урахуванням впливу сигнатур і відповідно до трафіку. Розрахунковий середній час глибокої перевірки пакетів використовується для визначення оптимального правила балансування навантаження, яке максимізує і / або збільшує кількість пакетів, які обробляються датчиками СВВ.

База даних сигнатур рідко змінюється під час виявлення вторгнень і варіюється при періодичному оновленні бази сигнатур. Однак сам трафік може бути значно змінений під час обслуговування, а правило балансування навантаження має варіюватися в залежності від відношення між сигнатурою і трафіком. Трафік визначається набором пакетів, які надходять, і зазвичай представляється у вигляді кількості даних до часу (наприклад, кБ/сек або МБ/сек). Якщо кількість вхідних пакетів збільшується, трафік також збільшується.

Для прискорення обробки пакетів і розподілу пакетів за потоками обробки пакетів використовується статичне хешування потоку. Статичні схеми хешування для аналізу полів заголовка мережного і транспортного рівнів визначають вузли СВВ для пересилання пакетів.

4. МЕТОД БАЛАНСУВАННЯ САМОПОДІБНОГО НАВАНТАЖЕННЯ

У даній роботі пропонується метод балансування навантаження, заснований на обслуговуванні з урахуванням часу балансування навантаження, аналізі сигнатур і обліку властивостей самоподібності трафіку. Самоподібність трафіку означає збереження закону розподілу при різних масштабах часу [10,14]. Ступінь самоподібності характеризується числом – показником Херста H $(0<H<1)$, який поряд з цим є мірою довгострокової залежності. Чим більше значення H, тим сильніше

ISSN 2663 - 4023

і довше кореляція між значеннями трафіку, саме ця властивість трафіку не дає ресурсам системи швидко звільнятися, оскільки за великими значеннями даних з великою ймовірністю також слідують великі [8, 14, 20].

Властивість берстності (неоднорідності трафіку) характеризується наявністю сильних викидів в реалізації трафіку при невеликій його інтенсивності. Для математичного опису берстності трафіку необхідно розглядати вибіркові моменти розподілу порядку q більше 2. У цьому випадку говорять про мультифрактальні властивості трафіку. Характеристикою мультифрактальних властивостей є узагальнений показник Херста $h(q)$ – нелінійна функція, яка заснована на моментах високого порядку q і характеризує неоднорідність самоподібного трафіку. Чим більше діапазон $\Delta h = h(q1) - h(q2)$, тим більше неоднорідність (берстність) трафіку, тобто тим сильніші викиди присутні в реалізації трафіку.

Для опису набору використаних сигнатур введемо набір $Sg = \{Sg_1, Sg_2, .., Sg_n\}$, де Sg_j – елементи набору сигнатур з бази даних сигнатур СВВ. Вторгнення в комп'ютерну систему представимо множиною $THR = \{THR_1, THR_2, .., THR_k\}$. Тоді набір правил реагування на передбачувані вторгнення можна позначити як $R = \{R_1, R_2, .., R_n\}$, де R_j є правилом зменшення або заборони відповіді на конкретний тип вторгнення j. Набір можна розділити на дві частини: правила першої частини дозволяють передавати пакети типу $R^+ = \{R_1, R_2, .., R_k\}$, що відповідні сигнатурам підмножини $Sg^+ = \{Sg_1, Sg_2, .., Sg_k\}$ набору Sg, а правила другій частини забороняють передачу пакетів типу $R^- = \{R_1, R_2, .., R_s\}$, які відповідні сигнатурам підмножини $Sg^- = \{Sg_1, Sg_2, .., Sg_s\}$ набору Sg, $R^+ \cap R^- = \varnothing$ та $Sg^+ \cap Sg^- = \varnothing$.

Час роботи T_{serv} означає середній час порівняння між сигнатурами Sg і одним або декількома пакетами з метою виявлення вторгнень THR. Кожен вузол порівнює один або кілька пакетів з однієї або декількома сигнатурами Sg_j. Чим більше сигнатур для порівняння, тим більше часу T_{serv} потрібно для аналізу, тобто час обслуговування пакета пропорційний кількості сигнатур.

Середній час обслуговування СВВ T_{serv}^{IDS} – це час, необхідний системі з конфігурацією правил $R(j)$ для успішного визначення дозволу або заборони реагування на певний тип вторгнення THR_j:

$$T_{serv}^{IDS} = \left[\sum_{j=1}^{N} P(j) \sum_{s=1}^{N} T_{serv}(\mathrm{s})\,\mathrm{R}^{-}(\mathrm{s})\right] + \left(1 - \sum_{j=1}^{N} P(j)\right) \times \sum_{j=1}^{N} T_{serv}(j)\,\mathrm{R}^{+}(j), \qquad (1)$$

де $P(j)$ - це ймовірність блокування правил $R(j)$; кожне правило $R(j)$ відповідає тільки за один тип шкідливих подій ; $T_{serv}(j)$ - час обслуговування пакета в j-му вузлу.

В даному методі використовується в якості одного з параметрів час глибокої перевірки пакетів. Час глибокої перевірки пакетів для одного пакета визначається кількістю сигнатур Sg_j відповідного пакета. Схему роботи методу балансування з урахуванням параметрів мультифрактального трафіку зображено на рис. 1.

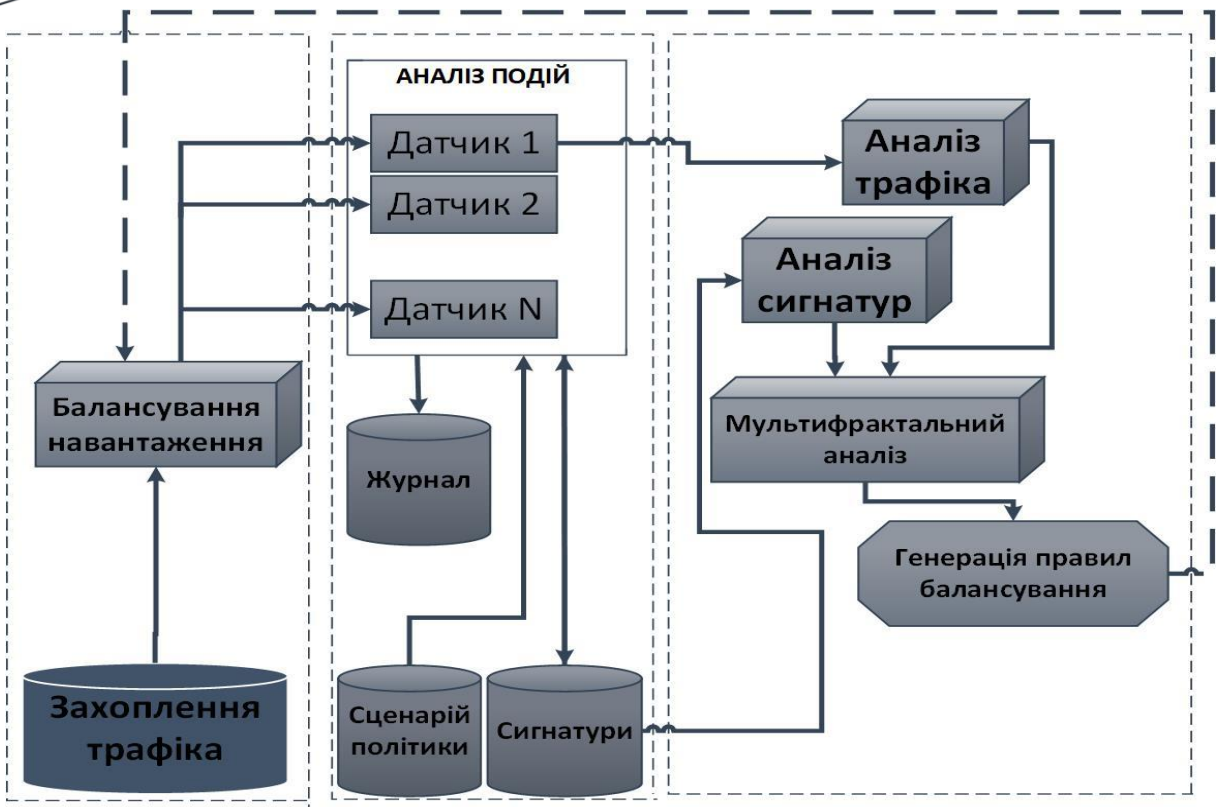

Рис. 1. Схема балансування навантаження в системі виявлення вторгнень, яка враховує мультифрактальні властивості трафіку

Нехай розглянута СВВ містить N вузлів $Nids_i$, $i=1,...,N$, кожен з яких приймає кілька незалежних потоків даних, які розподіляються між вузлами СВВ відповідно до політики формування трафіку в умовах обмежених ресурсів. Інформаційні потоки, що надходять до мережі, діляться на множину класів обслуговування $Z=\{z_{qs}\}$, $qs=1,...,m$. Для визначення стану навантаження вузлів і завантаженості СВВ необхідно збирати статистику вхідної черги за певний період часу $[t_0,t_0+T]$ і обчислювати загальні значення завантаження вузлів СВВ і системи в цілому.

Метод балансування в СВВ складається з наступних операцій:

1. Трафік, що надходить в СВВ, обробляється відповідно до процедури розподілу, яка класифікує його в потоки даних по qs-м типами послуг.

2. Для кожного потоку обчислюються наступні характеристики:

– мультифрактальні параметри;

– відношення кількості сигнатур для кожного qs-го типу потоку до загальної кількості сигнатур Sg;

– відношення кількості пакетів кожного qs-го типу до загальної кількості пакетів за певний період часу T;

– час порівняння пакетів з сигнатурою T_{serv}.

3. Розраховується середній час глибокої перевірки пакетів qs-го класу за формулою:

$$T_{new}^{qs} = \begin{cases} T_{serv}^{IDS}(\text{qs}), & H = 0,5; \\ T_{serv}^{IDS}(\text{qs}) + (H - 0,5)T_{serv}, & 0,5 < H < 0,9;\ \Delta h \le 0,4; \\ T_{serv}^{IDS}(\text{qs}) + (H - 0,5)(\Delta h - 0,4)T_{serv}, & 0,5 < H < 0,9;\ 0,4 < \Delta h < 1; \\ T_{serv}^{IDS}(\text{qs}) + T_{serv}, & H \ge 0,9 \text{ or } H > 0,5,\ \Delta h \ge 1, \end{cases}, \quad (2)$$

де $T_{serv}^{IDS}(qs)$ визначається відповідно до (1) для кожного класу обслуговування і з необхідними ресурсами. Оцінка середнього часу перевірки пакетів не змінюється ($T_{new}^{qs} = T_{serv}^{IDS}(qs)$), якщо трафік не має довгострокової залежності. При значеннях $0,5 < H < 0,9$ і малому діапазоні узагальненого показника Херста ($\Delta h \le 0,4$) значення T_{new}^{qs} збільшується пропорційно параметру Херста. Якщо трафік є персистентним ($0,5 < H < 0,9$) та існує велика берстність даних ($0,4 < \Delta h < 1$), то величина T_{new}^{qs} збільшується пропорційно обом параметрам Δh і H. Оцінка T_{new}^{qs} приймає максимальне значення $T_{serv}^{IDS}(\text{qs}) + T_{serv}$ якщо значення $H \ge 0,9$ або для персистентного трафіку ($H > 0,5$) з діапазоном значень узагальненого показника Херста $\Delta h \ge 1$.

4. На основі оцінки $T_{serv}^{IDS}(qs)$ створюється нове правило балансування навантаження, згідно з яким створюється список потоків qs -го типу, для яких $T_{new}^{qs} \ge T_{lev}$ і список потоків qs -го типу, для яких $T_{new}^{qs} < T_{lev}$, де T_{lev} - певний СВВ значення часу обробки пакетів, які призначені для обробки різними компонентами СВВ .

5. Балансування пакетів, які надійшли, здійснюється в наступному встановленому періоді часу $T + \Box T$ на компонентах СВВ, використовуючи знову правило балансування.

6. Балансування триває відповідно до п. 1-5.

Запропонований в даній роботі метод спрямований на забезпечення рівномірного балансування мультифрактального трафіку в дискретні моменти часу, щоб повною мірою використовувати багатоядерну / багатопотокову ємність, що призводить до більш ефективного використання системних ресурсів при обробці даних для виявлення вторгнень.

5. РЕЗУЛЬТАТИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Для аналізу якості роботи запропонованого методу було розроблено програмне забезпечення та проведено чисельні експерименти. Час обробки для всіх правил було вибрано рівним одній одиниці часу (одному такту роботи). На вхід системи подавався згенерований мультифрактальний трафік, що містив маркери загроз. Ці дані надходили на балансувальник, який регулював потоки даних за допомогою обраної політики балансування і відправляв до вузлів СВВ. В ході експериментів змінювалися параметри мультифрактальності трафіку Δh і H. У табл. 1 наведені значення показників продуктивності для стандартного методу балансування навантаження (СМ) і запропонованого методу (ЗМ) в залежності від значень параметрів мультифрактального вхідного трафіку. В якості показників продуктивності роботи балансувальника були обрані: кількість втрачених та непроаналізованих пакетів і величина дисбалансу системи, де дисбаланс це ступінь нерівномірності розподілу навантаження між

ISSN 2663 - 4023

серверами. Розрахунок величини дисбалансу комп'ютерної системи представлений в роботах [18, 23, 25, 26].

Таблиця 1

Показники продуктивності для стандартного методу балансування навантаження і запропонованого методу

Параметри мультифрактальності	Втрачені дані, %		Дисбаланс, %c		Непроаналізовані пакети, %	
	СМ	ЗМ	СМ	ЗМ	СМ	ЗМ
H=0,6, Δh=2	3.4	1.9	0.28	0.21	8.9	7.8
H=0,6, Δh=6	6.6	6.3	0.66	0.57	20	17.2
H=0,7, Δh=2	4.6	4	0.42	0.34	12.4	10.3
H=0,7, Δh=6	11	9.8	0.7	0.62	24.5	22
H=0,8, Δh=2	7.6	7.1	0.51	0.44	16	16
H=0,8, Δh=6	16.6	15.9	0.81	0.72	32.4	28
H=0,9, Δh=2	12.1	11.2	0.5	0.46	19	19
H=0,9, Δh=6	23.1	22	0.99	0.92	39.7	35.1

В результаті проведених досліджень показано, що характеристики мультифрактального трафіку істотно впливають на дисбаланс системи. Табл. 1 демонструє, що при збільшенні показника Херста H і діапазону узагальненого показника Херста Δh збільшується кількість не проаналізованих пакетів і втрачених даних та істотно збільшується дисбаланс системи.

При низьких значеннях параметрів самоподібності і берстності трафіку система балансування приходить в стан рівноваги. В цьому випадку ефективність СВВ є задовільною, а значення дисбалансу прагне до нуля. При великих значеннях параметра Херста і великій неоднорідності трафіку система балансування знаходиться в нестабільному стані і значення дисбалансу збільшується в кілька разів, що призводить до максимальному навантаженню ресурсів, і, отже, до значного збільшення кількості не проаналізованих пакетів і втрачених даних.

6. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У даній роботі пропонується новий підхід до вирішення задачі балансування самоподібного навантаження в високошвидкісних системах виявлення вторгнень. Запропоновано модифікований метод балансування навантаження, заснований на обліку часу обслуговування, в якому пакети, які надходять в заданий період часу, порівнюються з однією або декількома сигнатурами. Запропонований метод враховує характеристики мультифрактального трафіку для розрахунку часу глибокої перевірки пакетів, на основі якого обчислюється час, необхідний для порівняння пакета з сигнатурами, збирає статистику часу роботи, здійснює генерацію і оновлення правил балансування пакетів, які прибувають.

Результати чисельного моделювання показують, що даний метод балансування навантаження забезпечує рівномірний розподіл навантаження на вузлах СВВ. Це дозволяє забезпечити високу швидкість і точність визначення вторгнень при якісному балансуванні при самоподібному навантаженню.

У майбутній роботі планується провести порівняльний аналіз результатів роботи правил для виявлення вторгнень за допомогою сигнатур і аномальної поведінки для різних типів атак (відмова в обслуговуванні, підозріла активність, системні атаки), їх

вплив на фрактальні властивості трафіку. Також планується визначити баланс істинопозитивних та хибнопозитивних значень, щоб зменшити час виявлення вторгнень та ймовірність появи помилок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Q. Hu, S.-Y. Yu and M. R. Asghar, “Analysing performance issues of open-source intrusion detection systems in high-speed networks,” *Journal of Information Security and Applications*, Volume 51, 102426, April 2020. https://doi.org/10.1016/j.jisa.2019.102426

[2] J. Jabeza and B. Muthukumar Dr., “Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach,” *Procedia Computer Science*, Volume 48, pp. 338-346, 2015. https://doi.org/10.1016/j.procs.2015.04.191

[3] M. Hotaling. “IDS Load Balancer Security Audit: An Administrator's Perspective.” *SANS GIAC Systems and Network Auditor*Version 2.1, Option 1, SANS Institute 2004.

[4] S. Noel and S. Jajodia, “Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs,” *Journal of Network and Systems Management*, 16(3), pp.259-275, 2008. doi: 10.1007/s10922-008-9109-x

[5] H. Chen, J. A. Clark, S. Shaikh, H. Chivers and P. Nobles, “Optimising IDS Sensor Placement,” *Conference: ARES 2010*, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow. doi: 10.1109/ARES.2010.92

[6] Citrix ADC. (2019, January 6). “Use case 10: Load balancing of intrusion detection system servers”. [Online]. 05. Available: https://docs.citrix.com/en-us/netscaler/12/load-balancing/load-balancing-ids-servers.html [Jan. 30, 2020].

[7] Haproxy. (2019, Sept.) ALOHA load balancer Stateful firewalls, IPS, IDS and UTM load balancing. [Online]. 05. Available: https://www.haproxy.com/support/technical-notes/an-0062-en-stateful-firewalls-ips-ids-and-utm-load-balancing/ [Jan. 28, 2020].

[8] И.Н. Иванисенко, Л.О. Кириченко и Т.А. Радивилова. “Методы балансировки с учетом мультифрактальных свойств трафика,” *International journal “Information content and processing”*, Vol.2(4), pp.345-368, 2015.

[9] I. Ivanisenko and T. Radivilova, "The multifractal load balancing method," *2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology* (PIC S&T), Kharkiv, 2015, pp. 122-123.

[10] D. Ageyev, L. Kirichenko, T. Radivilova, M. Tawalbeh and O. Baranovskyi, "Method of self-similar load balancing in network intrusion detection system," *2018 28th International Conference Radioelektronika* (RADIOELEKTRONIKA), Prague, 2018, pp. 1-4. doi: 10.1109/RADIOELEK.2018.8376406

[11] M. Andreolini, S. Casolari, M. Colajanni and M. Marchetti, "Dynamic load balancing for network intrusion detection systems based on distributed architectures," *Sixth IEEE International Symposium on Network Computing and Applications* (NCA 2007), Cambridge, MA, 2007, pp. 153-160. doi: 10.1109/NCA.2007.17

[12] A. Le, D. R. Cheriton, R. Boutaba, R. Boutaba and E. Al-Shaer, “Correlation-based Load Balancing for Network Intrusion Detection and Prevention Systems,” *4th International ICST Conference on Security and Privacy in Communication Networks*, September 2008. doi: 10.1145/1460877.1460880

[13] Anh Le, E. Al-Shaer and R. Boutaba, "On optimizing load balancing of intrusion detection and prevention systems," *IEEE INFOCOM Workshops* 2008, Phoenix, AZ, 2008, pp. 1-6. doi: 10.1109/INFOCOM.2008.4544576

[14] Т.А. Радівілова, “Метод розподілу самоподібного навантаження в мережній системі виявлення вторгнень,” *Проблеми телекомунікацій*, №2(21), с.42-51, 2017.

[15] Premala and Bakhar, "MAC layer intrusion detection system by cooperation of cross layer in MANET," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing* (ICECDS), Chennai, 2017, pp. 2571-2574. doi: 10.1109/ICECDS.2017.8389918

[16] H. Jiang, G. Zhang, G. Xie, K. Salamatian and L. Mathy, "Scalable high-performance parallel design for Network Intrusion Detection Systems on many-core processors," *Architectures for Networking and Communications Systems*, San Jose, CA, 2013, pp. 137-146. doi: 10.1109/ANCS.2013.6665196

[17] Sireesha Rodda, Uma Shankar Rao Erothi, “Class imbalance problem in the Network Intrusion Detection Systems,” *2016 International Conference on Electrical, Electronics, and Optimization Techniques* (ICEEOT). 2016. DOI: 10.1109/ICEEOT.2016.7755181

[18] Ciza Thomas, “Improving intrusion detection for imbalanced network traffic,” *Security and communication Networks*, 6, 2013, pp. 309–324. doi: 10.1002/sec.564

[19] Y. Choi, WooJin Park, SeokHwan Choi and S. Seo, "STEAL: Service Time-Aware Load balancer on many-core processors for fast intrusion detection," *2016 IEEE Conference on Computer Communications Workshops* (INFOCOM WKSHPS), San Francisco, CA, 2016, pp. 65-70. doi: 10.1109/INFCOMW.2016.7562047

[20] L. Kirichenko and T. Radivilova, "Analyzes of the distributed system load with multifractal input data flows," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics* (CADSM), Lviv, 2017, pp. 260-264.

[21] T. Radivilova, L. Kirichenko and I. Ivanisenko, "Calculation of distributed system imbalance in condition of multifractal load," *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2016, pp. 156-158. doi: 10.1109/INFOCOMMST.2016.7905366

[22] Khor KC., Ting CY., Phon-Amnuaisuk S, "The Effectiveness of Sampling Methods for the Imbalanced Network Intrusion Detection Data Set," In: Herawan T., Ghazali R., Deris M. (eds) *Recent Advances on Soft Computing and Data Mining*. Advances in Intelligent Systems and Computing, vol 287. Springer, Cham. pp 613-622, 2014. DOI https://doi.org/10.1007/978-3-319-07692-8_58

[23] T. Radivilova, L. Kirichenko, D. Ageiev, V. Bulakh, "The Methods to Improve Quality of Service by Accounting Secure Parameters," In: Hu Z., Petoukhov S., Dychka I., He M. (eds) *Advances in Computer Science for Engineering and Education* II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, Springer, Cham, vol 938, pp 346-355. 2020. doi: https://doi.org/10.1007/978-3-030-16621-2_32

[24] Л.О. Кириченко, Т.А. Радивилова, И.Н. Иванисенко, "Анализ дисбаланса распределенной системы при самоподобной нагрузке," *Вісник Херсонського національного технічного університету*, №3(58). Херсон: ХНТУ, с.224-231, 2016.

[25] J. Lee and K. Park, "GAN-based imbalanced data intrusion detection system," *Personal and Ubiquitous Computing*, pp.1-8, 2019. https://doi.org/10.1007/s00779-019-01332-y

[26] D.A. Cieslak, N. V Chawla and A. Striegel, "Combating imbalance in network intrusion datasets," *Conference: 2006 IEEE International Conference on Granular Computing*, GrC 2006, Atlanta, Georgia, USA, May 10-12, 2006. doi: 10.1109/GRC.2006.1635905

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (7), 2020
ISSN 2663 - 4023

Tamara Radivilova
Ph.D, associated professor,
Kharkiv National University of Radio Electronics, V.V. Popovskyy department of infocommunication engineering, Kharkiv, Ukraine
ORCID ID: 0000-0001-5975-0269
tamara.radivilova@gmail.com

Lyudmyla Kirichenko
Dr., professor, professor of applied mathematics department
Kharkiv National University of Radio Electronics, department of applied mathematics, Kharkiv, Ukraine
ORCID ID: 0000-0002-2780-7993
lyudmila.kirichenko@nure.ua

Maksym Tawalbeh
Post graduate student V.V. Popovskyy department of infocommunication engineering, Kharkiv, Ukraine
Kharkiv National University of Radio Electronics, V.V. Popovskyy department of infocommunication engineering, Kharkiv, Ukraine
ORCID ID: 0000-0002-9629-4183
tavalbeh@icloud.com

Petro Zinchenko
Post graduate student of applied mathematics department
Kharkiv National University of Radio Electronics, department of applied mathematics, Kharkiv, Ukraine
ORCID ID: 0000-0002-9119-7720
petro.zinchenko@nure.ua

Vitalii Bulakh
Post graduate student of applied mathematics department
Kharkiv National University of Radio Electronics, department of applied mathematics, Kharkiv, Ukraine
ORCID ID: 0000-0002-9177-8787
bulakhvitalii@gmail.com

THE LOAD BALANCING OF SELF-SIMILAR TRAFFIC IN NETWORK INTRUSION DETECTION SYSTEMS

Abstract. The problem of load balancing in intrusion detection systems is considered in this paper. The analysis of existing problems of load balancing and modern methods of their solution are carried out. Types of intrusion detection systems and their description are given. A description of the intrusion detection system, its location, and the functioning of its elements in the computer system are provided. Comparative analysis of load balancing methods based on packet inspection and service time calculation is performed. An analysis of the causes of load imbalance in the intrusion detection system elements and the effects of load imbalance is also presented. A model of a network intrusion detection system based on packet signature analysis is presented. This paper describes the multifractal properties of traffic. Based on the analysis of intrusion detection systems, multifractal traffic properties and load balancing problem, the method of balancing is proposed, which is based on the funcsioning of the intrusion detection system elements and analysis of multifractal properties of incoming traffic. The proposed method takes into account the time of deep packet inspection required to compare a packet with signatures, which is calculated based on the calculation of the information flow multifractality degree. Load balancing rules are generated by the estimated average time of deep packet inspection and traffic multifractal parameters. This paper presents the simulation results of the proposed load balancing method compared to the standard method. It is shown that the load balancing method proposed in this paper provides for a uniform load distribution at the intrusion detection system elements. This allows for high speed and accuracy of intrusion detection with high-quality multifractal load balancing.

Keywords: load balancing; intrusion detection systems; self-similar traffic; information flows; deep packet inspection; attacks; load imbalance.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Q. Hu, S.-Y. Yu and M. R. Asghar, “Analysing performance issues of open-source intrusion detection systems in high-speed networks,” *Journal of Information Security and Applications*, Volume 51, 102426, April 2020. https://doi.org/10.1016/j.jisa.2019.102426

[2] J. Jabeza and B. Muthukumar Dr., “Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach,” *Procedia Computer Science*, Volume 48, pp. 338-346, 2015. https://doi.org/10.1016/j.procs.2015.04.191

[3] M. Hotaling. “IDS Load Balancer Security Audit: An Administrator's Perspective.” *SANS GIAC Systems and Network Auditor*Version 2.1, Option 1, SANS Institute 2004.

[4] S. Noel and S. Jajodia, “Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs,” *Journal of Network and Systems Management*, 16(3), pp.259-275, 2008. doi: 10.1007/s10922-008-9109-x

[5] H. Chen, J. A. Clark, S. Shaikh, H. Chivers and P. Nobles, “Optimising IDS Sensor Placement,” *Conference: ARES 2010*, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow. doi: 10.1109/ARES.2010.92

[6] Citrix ADC. (2019, January 6). “Use case 10: Load balancing of intrusion detection system servers”. [Online]. 05. Available: https://docs.citrix.com/en-us/netscaler/12/load-balancing/load-balancing-ids-servers.html [Jan. 30, 2020].

[7] Haproxy. (2019, Sept.) ALOHA load balancer Stateful firewalls, IPS, IDS and UTM load balancing. [Online]. 05. Available: https://www.haproxy.com/support/technical-notes/an-0062-en-stateful-firewalls-ips-ids-and-utm-load-balancing/ [Jan. 28, 2020].

[8] I. Ivanisenko, L. Kirichenko and T. Radivilova, “Balancing methods based on multifractal traffic properties,” *International journal “Information content and processing”*, Vol.2(4), pp.345-368, 2015.

[9] I. Ivanisenko and T. Radivilova, "The multifractal load balancing method," *2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology* (PIC S&T), Kharkiv, 2015, pp. 122-123.

[10] D. Ageyev, L. Kirichenko, T. Radivilova, M. Tawalbeh and O. Baranovskyi, "Method of self-similar load balancing in network intrusion detection system," *2018 28th International Conference Radioelektronika* (RADIOELEKTRONIKA), Prague, 2018, pp. 1-4. doi: 10.1109/RADIOELEK.2018.8376406

[11] M. Andreolini, S. Casolari, M. Colajanni and M. Marchetti, "Dynamic load balancing for network intrusion detection systems based on distributed architectures," *Sixth IEEE International Symposium on Network Computing and Applications* (NCA 2007), Cambridge, MA, 2007, pp. 153-160. doi: 10.1109/NCA.2007.17

[12] A. Le, D. R. Cheriton, R. Boutaba, R. Boutaba and E. Al-Shaer, “Correlation-based Load Balancing for Network Intrusion Detection and Prevention Systems,” *4th International ICST Conference on Security and Privacy in Communication Networks*, September 2008. doi: 10.1145/1460877.1460880

[13] Anh Le, E. Al-Shaer and R. Boutaba, "On optimizing load balancing of intrusion detection and prevention systems," *IEEE INFOCOM Workshops* 2008, Phoenix, AZ, 2008, pp. 1-6. doi: 10.1109/INFOCOM.2008.4544576

[14] T. Radivilova “Method of self-similar load distribution in network intrusion detection system,” *Problemy telekomunikatsiy*, №2(21), pp.42-51, 2017.

[15] Premala and Bakhar, "MAC layer intrusion detection system by cooperation of cross layer in MANET," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing* (ICECDS), Chennai, 2017, pp. 2571-2574. doi: 10.1109/ICECDS.2017.8389918

[16] H. Jiang, G. Zhang, G. Xie, K. Salamatian and L. Mathy, "Scalable high-performance parallel design for Network Intrusion Detection Systems on many-core processors," *Architectures for Networking and Communications Systems*, San Jose, CA, 2013, pp. 137-146. doi: 10.1109/ANCS.2013.6665196

[17] Sireesha Rodda, Uma Shankar Rao Erothi, “Class imbalance problem in the Network Intrusion Detection Systems,” *2016 International Conference on Electrical, Electronics, and Optimization Techniques* (ICEEOT). 2016. DOI: 10.1109/ICEEOT.2016.7755181

[18] Ciza Thomas, “Improving intrusion detection for imbalanced network traffic,” *Security and communication Networks*, 6, 2013, pp. 309–324. doi: 10.1002/sec.564

[19] Y. Choi, WooJin Park, SeokHwan Choi and S. Seo, "STEAL: Service Time-Aware Load balancer on many-core processors for fast intrusion detection," *2016 IEEE Conference on Computer Communications Workshops* (INFOCOM WKSHPS), San Francisco, CA, 2016, pp. 65-70. doi: 10.1109/INFCOMW.2016.7562047

[20] L. Kirichenko and T. Radivilova, "Analyzes of the distributed system load with multifractal input data flows," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics* (CADSM), Lviv, 2017, pp. 260-264.

[21] T. Radivilova, L. Kirichenko and I. Ivanisenko, "Calculation of distributed system imbalance in condition of multifractal load," *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkiv, 2016, pp. 156-158. doi: 10.1109/INFOCOMMST.2016.7905366

[22] Khor KC., Ting CY., Phon-Amnuaisuk S, "The Effectiveness of Sampling Methods for the Imbalanced Network Intrusion Detection Data Set," In: Herawan T., Ghazali R., Deris M. (eds) *Recent Advances on Soft Computing and Data Mining*. Advances in Intelligent Systems and Computing, vol 287. Springer, Cham. pp 613-622, 2014. DOI https://doi.org/10.1007/978-3-319-07692-8_58

[23] T. Radivilova, L. Kirichenko, D. Ageiev, V. Bulakh, "The Methods to Improve Quality of Service by Accounting Secure Parameters," In: Hu Z., Petoukhov S., Dychka I., He M. (eds) *Advances in Computer Science for Engineering and Education* II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, Springer, Cham, vol 938, pp 346-355. 2020. doi: https://doi.org/10.1007/978-3-030-16621-2_32

[24] L. Kirichenko, T. Radivilova, I. Ivanisenko, "Distributed system imbalance analysis under self-similar load," *Visnyk Khersons'koho natsional'noho tekhnichnoho universytetu*, №3(58), pp.224-231, 2016.

[25] J. Lee and K. Park, "GAN-based imbalanced data intrusion detection system," *Personal and Ubiquitous Computing*, pp.1-8, 2019. https://doi.org/10.1007/s00779-019-01332-y

[26] D.A. Cieslak, N. V Chawla and A. Striegel, "Combating imbalance in network intrusion datasets," *Conference: 2006 IEEE International Conference on Granular Computing*, GrC 2006, Atlanta, Georgia, USA, May 10-12, 2006. doi: 10.1109/GRC.2006.1635905