УДК 004.056.5

МЕТОД РОЗПОДІЛУ САМОПОДІБНОГО НАВАНТАЖЕННЯ В МЕРЕЖНІЙ СИСТЕМІ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Т.А. РАДІВІЛОВА
Харківський національний університет радіоелектроніки

Abstract *– The paper considers the problem of load balancing in network intrusion detection systems. Load balancing method that is multi-components of network intrusion detection and analysis of multifractal properties of incoming traffic is proposed. The proposed method takes into account the degree of multifractality to calculate the time of deep packet inspection based on which the time required to compare the package of signatures is calculated. The load balancing rules are generated using the estimated average time of deep packet inspection and the multifractal parameters of input load. For the analysis of the proposed load balancing method a simulation of the balancing system was conducted in a program written in Python. Numerous studies of the balancing of the network intrusion detection system at various values of the parameters of multifractal traffic have been carried out. Numerous studies of balancing the network intrusion detection system with different values of parameters of multifractal traffic were conducted. A comparative analysis of the proposed load balancing method with a standard balancing method was performed using simulations. It is shown that the proposed method improves the quality of service and reduces the percentage of packets that have not been tested for intrusion detection.*

Анотація *– У роботі розглянута проблема балансування навантаження в мережних системах виявлення вторгнень. Запропоновано метод балансування вхідного мультифрактального трафіку серед кількох компонент мережних систем виявлення вторгнень. За допомогою імітаційного моделювання проведено порівняльний аналіз запропонованого методу балансування навантаження зі стандартним методом балансування, який показав, що запропонований метод покращує якість обслуговування і знижує відсоток пакетів, які не пройшли перевірку на виявлення вторгнень.*

Аннотация *– В работе рассмотрена проблема балансировки нагрузки в сетевых системах обнаружения вторжений. Предложен метод балансировки входящего мультифрактального трафика среди нескольких компонент сетевых систем обнаружения вторжений. С помощью имитационного моделирования проведен сравнительный анализ предлагаемого метода балансировки нагрузки со стандартным методом балансировки, который показал, что предлагаемый метод улучшает качество обслуживания и снижает процент пакетов, которые не прошли проверку на выявление вторжений.*

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 (Intrusion Detection System/Intrusion Prevention System, IDS/IPS) – це необхідний елемент захисту від мережних атак. Ос-

новним призначенням подібних систем є виявлення фактів несанкціонованого доступу до корпоративної мережі і прийняття відповідних заходів протидії.

Система виявлення вторгнень мережі зазвичай розташовується у периметрі мережі або у її відносно важливих сегментах, щоб відстежувати різні пакети даних в мережі. Вузьким місцем, що впливає на продуктивність мережі, є швидкість обробки мережного пристрою безпеки [1]. Система виявлення вторгнень в мережі фіксує кожен пакет даних в мережі і вимагає багато часу і системних ресурсів для аналізу і зіставлення пакета даних функції будь-якого типу атаки. Мережні IDS (Network Intrusion Detection System, NIDS) можуть не виконувати повний аналіз при високих навантаженнях, однак це може привести до того, що деякі атаки не будуть виявлені [2, 3]. 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 трафік має самоподібні характеристики і великі викиди, що викликає серйозний дисбаланс навантаження при статичних правилах балансування між розподіленими датчиками, що може привести до втрати пакетів [4, 5]. Отже, розподілена архітектура NIDS повинна поєднуватися з адекватними динамічними механізмами перерозподілу навантаження. Таким чином, критичною проблемою є розробка методу балансування самоподібного навантаження для підвищення пропускної здатності мережної системи виявлення вторгнень.

В даний час існують роботи, спрямовані на вирішення проблеми балансування навантаження в NIDS. В роботі [6] розглянуто паралельну архітектуру NIDS, яка долає обмеження на виявлення вторгнення, розподіляючи навантаження мережного трафіку за масивом вузлів датчиків. Вона також використовує динамічний зворотній зв'язок від вузлів датчика для адаптації до змін мережного трафіку. В роботі [7] пропонується загальна архітектура для розгортання NIDS в мережі, яка використовує три можливості масштабування: розподіл за шляхом для поділу обов'язків, репліку-вання трафіку в кластери NIDS і агрегування проміжних результатів для поділу дорогої обробки NIDS.

В роботі [3] пропонуються різні політики активації / деактивації динамічного балансувальника навантаження шляхом порівняння одиночних і подвійних порогових схем та подання навантаження на основі моделей ресурсів і моделей агрегації навантаження.

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

I. Опис мережної системи виявлення вторгнень

Система виявлення вторгнень являє собою комбінацію програмного і апаратного забезпечення для виявлення вторгнень. IDS можна класифікувати за типом хосту і

мережі, що зумовлено різними підходами до категоризації подій безпеки, атак і вторгнень [1, 3].

1. Система виявлення вторгнень хосту є прикладом програмної реалізації продукту і встановлюється на одну машину, отже детектує атаки, які відносяться тільки до цієї машини. Як джерело даних зазвичай використовує системні журнали, журнали додатків і т. д. Перевага систем такого типу в тому, що знаходячись на машині, вони бачать всю її внутрішню структуру і можуть контролювати і перевіряти набагато більше об'єктів, не тільки зовнішній трафік.

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.

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

У базовому сценарії розподілу трафік рівномірно розподіляється між кожним датчиком NIDS в кластері. Це означає, що кожен датчик NIDS повинен отримувати рівний обсяг трафіку. З такими пристроями, як балансувальник навантаження NIDS і перемикачі сьомого рівня моделі OSI, трафік можна відфільтрувати до його відправки до кластеру NIDS [8, 9].

Кращою альтернативою виконання базового рівномірного розподілу з'єднань з кожним NIDS є метод, де деякі NIDS отримують тільки певні типи трафіку. Наприклад, якщо кластер NIDS містив чотири фізичні NIDS, один з NIDS буде спостерігати тільки за HTTP-трафіком, другий – тільки за SMTP-трафіком, третій буде спостерігати тільки за трафіком FTP, а четвертий NIDS – тільки за DNS і RPC-трафіком. Це дозволить налаштувати кожну NIDS, щоб вони шукали тільки певні типи сигнатур і аномалій атаки [8]. Отже кожна NIDS 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 незбалансований (HTTP - 47%, UDP - 37%, HTTP video - 9%, VoIP - 1%) [10]

Через те, що архітектура, заснована тільки на одному датчику трафіку, не може бути достатньою для того, щоб протистояти уразливостям 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 балансувальником і набором датчиків, які направляють частини мережного трафіку різних датчиків NIDS через деяку політику формування трафіку [9, 11].

Кожен датчик NIDS аналізує отриманий трафік на наявність вторгнень. Основна проблема полягає в тому, що вхідний трафік, що надходить до розподіленої архітектури NIDS, володіє довгостроковою залежністю і сплесками. Тому в роботі використовується аналіз вхідного трафіку на наявність фрактальних властивостей і динамічний перерозподіл навантаження між датчиками [12]. Для цього пропонується використовувати балансувальник, який отримує періодичну інформацію про стан датчиків, і на основі деякої політики він може здійснювати механізм балансування навантаження для переміщення частини мережного трафіку з перевантажених датчиків на менш навантажені. 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 для процесу балансування навантаження. [12]

У кожен момент часу $t \in [t_0, t_0 + T]$, де t_0 – це початок періоду T, на вхід NIDS надходять потоки трафіку інтенсивністю $\lambda = [\lambda_1, \lambda_2, .., \lambda_\sigma]$, σ - множина потоків, що відносяться до qs-го класу обслуговування, які необхідно доставити на i-й вузол $Nids_i$ для обробки або подальшої передачі, не перевищуючи заданих максимально допустимих значень затримки τ_{qs} і максимально допустимих значень втрат p_{qs} в залежності від пропускної здатності і поточного завантаження вузлів в конкретний момент часу.

Трафік має множину характеристик $V = \{\lambda, h, S_t\}$, де $h = [H, h(q), \Delta h]$, де $h(q)$ - вибіркове значення функції узагальненого показника Херста, параметр $-10 \le q \le 10$, $H = h(2)$ – значення параметру Херста, $\Delta h = h(q_{\min}) - h(q_{\max})$ – діапазон значень узагальненого показника Херста для ділянки трафіку; множина $S_t = \{st_1, st_2, ...\}$ збирає інформацію про мережний трафік NIDS, де st може відповідати мережна адреса, порт, адреса пристрою, ідентифікатор протоколів, розмір поля пакета тощо.

Для опису набору сигнатур, що використовуються, представлено набір $Sg = \{Sg_1, Sg_2, .., Sg_n\}$, де $Sg_n, n \ge 0$ – це елементи набору сигнатур з бази даних сигнатур NIDS. Тоді набір правил для відповіді на NIDS про передбачувані вторгнення $R = \{R_1, R_2, .., R_j\}$, де $R_j, j \ge 0$ – це правила, що дозволяють/забороняють відповідь на певний тип вторгнення, можна розділити на дві частини. Правила, що дозволяють передавати пакети $R^+ = \{R_1, R_2, ...\}$ типу, що відповідають сигнатурам з підмножини $Sg^+ = \{Sg_1, Sg_2, ..\}$ набору Sg, і правила, які забороняють передавати пакети $R^- = \{R_1, R_2, ...\}$ типу, відповідні сигнатурам з підмножини $Sg^- = \{Sg_1, Sg_2, ...\}$ набору $R^+ \cap R^- = \varnothing$ та $Sg^+ \cap Sg^- = \varnothing$.

Вхідний вузол $Nids_i$ отримує декілька незалежних мультифрактальних потоків пакетів з різною інтенсивністю, які розподіляються між вузлами відповідно до полі-

тики формування трафіку в обмежених чергах Q_i [8, 9]. Система NIDS містить N ($i=\overline{1,N}$) вузлів, кожен з них має свою чергу, а також одну чергу на вході.

Для визначення стану навантаження вузла NIDS необхідно збирати статистику вхідної черги за певний період часу T.

Середня завантаженість i-го процесора NIDS вузла це CPU_i^u, u – кількість ЦПУ на i-му сервері. Аналогічним чином, середнє значення використання пам'яті – RAM_i^r, доступна пропускна здатність каналу до i-го вузла NIDS – це Net_i^k.

Сумарні значення дисбалансу всіх вузлів NIDS визначаються як: $IMB_{tot}=\frac{1}{N}\sum_{i=1}^{N} IMB_i$, коли значення дисбалансу i-х вузлів NIDS –

$$IMB_i = K_u(CPU_i^u - CPU_u^{All})^2 + K_r(RAM_i^r - RAM_r^{All})^2 + K_k(Net_i^k - Net_k^{All})^2,$$

де CPU_u^{All} є середнє значення використання всіх процесорів в системі, RAM_r^{All} – це середнє значення використання всієї пам'яті, Net_k^{All} – середня доступна пропускна здатність каналів у системі, параметри K_u, K_r, K_k позначають вагові коефіцієнти для процесора, пам'яті та доступної смуги пропускання мережі відповідно, які обираються експериментально таким чином, що $K_u + K_r + K_k = 1$ і залежать від виконуваних завдань та структури системи.

Час обслуговування пакетів T_{serv} відноситься до часу роботи, протягом якого проводиться порівняння між сигнатурами $Sg=\{Sg_1, Sg_2, .., Sg_n\}$ та одним або кількома пакетами для виявлення вторгнення $THR=\{\mathrm{THR}_1, \mathrm{THR}_2, .., \mathrm{THR}_k\}$. Кожен вузол порівнює кожен або кілька пакетів з одним або кількома сигнатурами Sg. Чим більше підписів присутні для порівняння, тим більше часу T_{serv} потрібно для аналізу. Іншими словами, час служби пакетів пропорційний кількості сигнатур, які повинні бути порівняні з пакетом. Співвідношення часу обслуговування пакету в одному вузлі до загального часу обслуговування пакету для операції на всіх вузлах називається швидкістю передачі пакетів.

Середній час служби IDS – це час, необхідний IDS з конфігурацією правил R_j для успішного визначення дозволу/заборони реагування на певний тип вторгнення. Середній час служби IDS визначається як [15]:

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

де $P(j)$ – це ймовірність блокування правил R_j; кожне правило R^{-} відповідає лише за один тип зловмисних подій.

Метод балансування навантаження використовує глибокий час огляду пакетів (DPI) вузла NIDS, в якому аналізується зв'язок між трафіком та сигнатурою за допомогою розрахованого часу обслуговування пакету. Час DPI для одного пакету визначається кількістю сигнатур, що відповідають пакету.

II. Запропонований метод балансування навантаження

У цій статті пропонується метод балансування навантаження, який базується на часі балансування навантаження, аналізі сигнатур, а також враховує властивості самоподібного трафіку. Самоподібність трафіку означає збереження закону розподілу за різними масштабами часу [10, 13, 14]. Ступінь самоподібності характеризується числом - показником Херста H ($0 < H < 1$), що також є мірою довготривалої залежності. Чим більше значення H, тим сильніше та довше кореляція між значеннями трафіку, ця властивість трафіку не дозволяє швидко звільняти системні ресурси [12].

Властивість берстності (неоднорідність трафіку) характеризується наявністю великих викидів (берстність) в реалізації трафіку з невеликою інтенсивністю. Для математичного опису властивості берстності необхідно розглянути q-ті моменти ($q > 2$) процесу. Характеристика мультифрактальних властивостей трафіку - це узагальнений показник Херста $h(q)$. Це нелінійна функція, яка базується на q-их моментах і характеризує неоднорідність самоподібного трафіку. Чим більше діапазон $\Delta h = h(q_{\min}) - h(q_{\max})$, тим більша гетерогенність (сплески) трафіку, тобто більш сильні викиди присутні в реалізації трафіку. Метод, запропонований в цій роботі, може забезпечити рівномірний розподіл навантаження на дискретних моментах для повного використання багатопотокових NIDS, що призводить до більш ефективного використання системи при обробці даних для виявлення вторгнення. Цей метод складається з наступних операцій.

1. Клієнти отримують велику кількість потоків інтенсивністю λ, які належать до qs-ого класу обслуговування. Вхідні дані мають множину характеристик $V = \{\lambda, h, S_t\}$ і обов'язково містять тип протоколу (TCP, UDP та ін.) та властивості протоколу. Властивості протоколу пакету даних містять вихідну IP-адресу, порт джерела, IP-адресу призначення та порт призначення.

2. Пакети, що надходять, балансуються на вузли відповідно до їх швидкості прибуття $T_{serv} / T_{serv}^{IDS}$ протягом певного періоду часу T. Балансування може застосовуватися для будь-якого обраного алгоритму [16]. Вхідні пакети обробляються процедурою розбивки, яка класифікує їх у потоки типу даних за типом послуги, визначаючи заголовки пакетів, що надходять, відповідно до типу та властивостей протоколу.

3. Для кожного потоку розраховуються мультифрактальні параметри $\Delta h, H$, а також співвідношення кількості сигнатур або кожного qs-го типу потоку до загальної кількості підписів Sg.

4. Балансувальник аналізує вхідні пакети в задані періоди часу T. Розраховується співвідношення кількості пакетів для кожного qs-го типу послуги до загальної кількості пакетів, що надходять протягом певного періоду часу. Далі балансувальник оцінює час порівняння пакетів з підписом T_{serv} та періодом обробки для певної послуги на основі параметрів мультифрактальності та співвідношення кількості сигнатур для кожного типу потоку до загальної кількості сигнатур Sg.

5. Процедура виявлення вторгнення виконується відповідно до набору сигнатур Sg. Тобто балансувальник навантаження порівнює принаймні одну з сигнатур з навантаженням пакетів, що надходять, принаймні одного типу послуги.

6. Оцінюється середній час пакетів DPI $T_{serv}^{IDS}(\text{qs})$, що відповідають конкретному обслуговуванню. Середній час DPI пакетів для сигнатур певної послуги може бути розрахований з використанням номера підпису та середнього часу обробки всіх сигнатур певної послуги з урахуванням параметрів мультифрактальності.

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

де $T_{serv}^{IDS}(\text{qs})$ визначається відповідно до класу обслуговування та необхідних ресурсів, значення $T_{serv}^{IDS}(\text{qs})$ обчислюється залежно від номера сигнатури. Оцінка середнього часу DPI пакетів не змінюється ($T_{new}^{qs} = T_{serv}^{IDS}(\text{qs})$), якщо трафік є звичайним Пуасонівським потоком ($H = 0,5$). За допомогою значення $0,5 < H < 0,9$ та низької дисперсії даних ($\Delta h \le 0,4$) значення $T_{serv}^{IDS}(\text{qs})$ збільшується пропорційно значенню індексу Херста. Коли значення параметра Херста $0,5 < H < 0,9$ та високі значення дисперсії даних ($0.4 < \Delta h < 1$) значення $T_{serv}^{IDS}(\text{qs})$ зростають пропорційно до обох параметрів. Оцінка середнього часу DPI пакетів з максимальним значенням $T_{serv}^{IDS}(\text{qs}) + T_{serv}$ обчислюється для значення $H \ge 0,9$ або для персистентного трафіку ($H > 0,5$) з діапазоном значень узагальненого показника Херста $\Delta h \ge 1$. Крім того, середній час обробки всіх підписів може відображатися як вага при оцінюванні середнього часу DPI.

7. Створюється перший список обслуговування, який має середнє значення DPI, що перевищує або дорівнює заданому рівню, шляхом сортування. Генерується другий список обслуговування, який має середній час менше, ніж заданий рівень.

8. Ініціюється зміна правила балансування. Зміна відбувається, коли виконується певна умова, яка впливає на загальний об'єм DPI розподіленої NIDS, або закінчується вказаний час для оновлення бази даних сигнатур.

9. Записуються статистичні дані про час виконання, які необхідні для порівняння підписів з пакетом для кожного типу послуги.

10. Створюється нове правило балансування навантаження $Load_T(T_{new}^{qs}, \text{H}, \Delta\text{h})$ на основі оцінки середнього часу DPI $T_{serv}^{IDS}(\text{qs})$. Воно може періодично змінюватися залежно від результату аналізу трафіку. Відповідно до нового правила балансування навантаження, пакети для кожного типу послуг, що входять до першого списку обслуговування, призначаються для обробки на деяких компонентах NIDS, а пакети

для типів обслуговування, включених до другого списку, призначаються для обробки на інших компонентах NIDS [16].

11. Після аналізу підпису оновлюється правило балансування навантаження. Балансування навантаження виконується відповідно до оновленого правила балансування навантаження $Load_T$.

12. Балансування прибуваючих пакетів виконується в наступний встановлений період часу 2T на декількох компонентах NIDS, використовуючи новостворене правило балансування, яке базується на результаті аналізу пакетів, що надходять за певний період часу T.

13. Події, що перевищують певний рівень трафіку вхідних пакетів або закінчення вказаного часу балансування навантаження, контролюються перед аналізом пакетів, що надходять у період часу 2T. Пакети обробляються та аналізуються компонентами NIDS, що використовують оновлене правило балансування навантаження.

14. Виконується балансування відповідно до операцій 2-13.

Таким чином, в роботі наведено метод балансування навантаження в мережній IDS, що враховує властивості самоподібного вхідного трафіку.

III. Результати експериментів

Імітаційне моделювання виконувалось в програмі, що написана на мові Python, для перевірки коректності роботи запропонованого методу. Під час моделювання ми призначили рівний час обробки для всіх правил (один блок часу). На вхід системи подавався згенерований мультифрактальний трафік, що описано у [4]. Дані, що надходять із зовнішньої мережі, створюють додатковий мультифрактальний трафік, що містить маркери загроз. Ці дані надсилаються до балансувальника, який регулює потік даних за допомогою обраної політики балансування та надсилається до вузлів NIDS. Для аналізу запропонованого методу балансування були проведені численні дослідження системи балансування NIDS для різних значень параметрів мультифрактального трафіку: діапазон значень узагальненого показника Херста $1,5 \le \Delta h \le 6$, значення параметра Херста $0,6 \le H \le 0,9$ та інтенсивності потоку застосування $0,5 \le \lambda \le 1$. У таблиці 1 показані значення показників ефективності для стандартного методу балансування навантаження (СМ) та запропонованого методу (ЗМ) для різних значень параметрів мультифрактальності вхідного трафіку.

Дослідження показали, що мультифрактальні характеристики трафіку істотно впливають на дисбаланс системи, кількість не проаналізованих пакетів і втрачених даних збільшується, як показано в табл. 1. При невеликих значеннях H і малої неоднорідності система балансування приходить в рівноважний стан і продуктивність NIDS задовільна, а значення дисбалансу прямує до нуля. При великих значеннях індексу Херста і великій неоднорідності система балансування знаходиться в нестійкому стані, а значення дисбалансу змінюється кілька разів, що призводить до максимального навантаження ресурсів і, отже, до значного збільшення кількості не проаналізованих пакетів і втрачених даних.

Таблиця 1. Зміна значень показників ефективності в залежності від параметрів мультифрактальності

Параметри трафіку	Втрачені пакети, %		IMB		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

Висновки

В роботі описано новий підхід до вирішення проблеми балансування самоподібного навантаження в високошвидкісних системах виявлення вторгнень. Пропонується модифікований метод балансування навантаження, заснований на обліку часу обслуговування, в якому пакети, що надходять в зазначений період часу, порівнюються з однією або декількома сигнатурами. Метод враховує ступінь мультифрактальності трафіку для обчислення часу DPI, на основі якого обчислюється час, необхідний для порівняння пакета з сигнатурами, збирає статистику робочого часу, генерує і оновлює правила для балансування вхідних пакетів. Результати імітаційного моделювання показали, що параметри мультифрактальності мають великий вплив на значення показників якості обслуговування. Чим більші значення параметрів мультифрактальності та неоднорідності вхідного трафіку, тим складніше його рівномірно розподілити. Запропонований метод балансування навантаження забезпечує статично рівномірний розподіл навантаження на вузлах NIDS, низький відсоток втрачених даних і не проаналізованих пакетів і спрямований на забезпечення високої швидкості і точності виявлення вторгнень при якісному балансуванні вхідного навантаження.

В подальшому планується провести порівняльний аналіз результатів роботи правил виявлення вторгнень за підписами і аномальною поведінкою для різних типів атак (відмова в обслуговуванні, підозріла діяльність, системна атака), їх вплив на мультифрактальні характеристики трафіку і визначення граничних значень для характеристик поведінки вхідних даних для зниження ймовірності виявлення помилок.

Список літератури:

1. *Mukherjee B.* Network intrusion detection / B. Mukherjee, L.T. Heberlein, K.N. Levitt // IEEE Network. – May-June 1994. – Vol. 8, No. 3. – P. 26-41.

2. *Warrender C.* Detecting intrusions using system calls: alternative data models. / C. Warrender, S. Forrest, B. Pearlmutter // Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No.99CB36344). – Oakland, CA, 1999. – P. 133-145.

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

4. *Ivanisenko I.* Investigation of self-similar properties of additive data traffic. / I. Ivanisenko, L. Kirichenko, T. Radivilova // 2015 Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT). – Lviv, 2015. – P. 169-171.

5. *Ageyev D.* LTE EPS network with self-similar traffic modeling for performance analysis. / D. Ageyev, N. Qasim // 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). – Kharkiv, 2015. – P. 275-277.

6. *Ageyev D.* Parametric Synthesis of Overlay Networks with Self-Similar Traffic. / D. Ageyev, M. Salah // Telecommunications and Radio Engineering. – 2016. – Vol. 75, No. 14. – P. 1231-1241.

7. *Schaelicke L.* SPANIDS: A Scalable Network Intrusion Detection Loadbalancer. / Lambert Schaelicke, Kyle Wheeler, Curt Freeland // Proceeding CF '05 Proceedings of the 2nd conference on Computing frontiers. – 2005. – P. 315-322.

8. *Heorhiadi V.* New Opportunities for Load Balancing in Network-Wide Intrusion Detection Systems. / Victor Heorhiadi, Michael K. Reiter, Vyas Sekar // Proceeding CoNEXT '12 Proceedings of the 8th international conference on Emerging networking experiments and technologies. – 2012. – P. 361-372. DOI: 10.1145/2413176.2413218.

9. *Li Xiao-Qian*. Load balancing method for Network Intrusion Detection. / Xiao-Qian Li, Tom Chen. // United States Patent Application Publication, US 2010/0246592 A1 – Sep. 30, 2010.

10. *Choi Yoon-ho*. Load balancing method and apparatus in Intrusion Detection Sysytem. / Yoon-ho Choi, Seung-Woo Seo, Bon-Hyun Koo, Hye-Jung Cho // United States Patent Application Publication, US 2017/0295191 A1 – Oct. 12, 2017.

11. *Erramilli A.* Self-similar traffic and network dynamics. / A. Erramilli, M. Roughan, D. Veitch, W. Willinger // Proceedings of the IEEE. – May 2002. – Vol. 90, No. 5. – P. 800-819. DOI: 10.1109/JPROC.2002.1015008.

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

13. *Ivanisenko I.* The multifractal load balancing method. / I. Ivanisenko, T. Radivilova // 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). – Kharkiv, 2015. – P. 122-123.

14. *Kirichenko L.* Dynamic load balancing algorithm of distributed systems. / L. Kirichenko, I. Ivanisenko, T. Radivilova // 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). – Lviv, 2016. – P. 515-518.

15. *Alsubhi K.* Performance analysis in Intrusion Detection and Prevention Systems. / K. Alsubhi, N. Bouabdallah, R. Boutaba // 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops. – Dublin, 2011. – P. 369-376.

16. *Ying Yu.* A Dynamic Forecast Load-balancing Algorithm for High-speed. Network Instruction Detection System. / Yu Ying, Deng Qidong.// 2012 International Conference on Image, Vision and Computing (ICIVC 2012), IPCSIT. – 2012. – Vol. 50. – P.1-7.