УДК 004.056.57

А.К. ЯЦЕНКО, В.І. ДУБРОВІН, Л.Ю. ДЕЙНЕГА
Національний університет «Запорізька політехніка»

АНАЛІЗ ТРАФІКУ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ЕНТРОПІЇ

Програмно-визначена мережа (SDN) – це підхід до створення мережі, яка використовує програмні контролери або інтерфейси прикладного програмування (API) для зв'язку з базовою апаратною інфраструктурою та напрямком трафіку в мережі замість фізичних маршрутизаторів і комутаторів.

Програмно-визначені мережі використовують централізований контролер, тому забезпечення надійності його роботи має дуже важливе значення для функціонування мережі.

Питання безпеки стає особливо гострим, коли кількість користувачів мережі зростає. Однією з найбільших і найпоширеніших загроз для програмно-визначених мереж є атака розподіленої відмови в обслуговуванні (DDoS).

Щоб виявити мережеві атаки, можна використовувати статистичні характеристики мережевого трафіку, такі як середнє значення вибірки, дисперсія вибірки, критерій хі-квадрат Пірсона та теоретико-інформаційна міра – ентропія. Кількісно ентропія характеризується за допомогою ентропії розподілу ймовірностей К. Шеннона.

Інформаційна ентропія – це міра невизначеності, пов'язана з випадковою величиною. Ентропія характеризує ймовірність, з якою встановлюється той чи інший стан, є мірою хаотичності чи незворотності. Чим більша хаотичність системи, тим вище значення ентропії, і навпаки.

Програмні комплекси базуються на основі ентропійного аналізу мережевих даних, записаних датчиками NetFlow. Типові датчики підключаються до портів TAP або SPAN на комутаторах. Потоки аналізуються протягом фіксованих інтервалів часу. Зібрані потоки реєструються в базі даних, а потім аналізуються. Фільтри аномалій передбачені за напрямком, протоколом і підмережею. Далі розраховується значення ентропії додатних і від'ємних значень α для розподілу характеристик руху.

На етапі виявлення спостережувана ентропія порівнюється з мінімальними та максимальними значеннями, що зберігаються в профілі, і визначається поріг аномалії. Порогові значення менше 0 або більше 1 вказують на ненормальну концентрацію або дисперсію відповідно.

Одним із рішень для виявлення таких атак є використання ентропії синтезу. Цей метод дозволяє виявляти DDoS-атаки за час, близький до реального, а значення ентропії для нормального і шкідливого трафіку відрізняються на 90%.

Ключові слова: виявлення аномалій, ентропія, мережевий потік, вимірювання мережевого трафіку, програмно визначена мережа, DDoS-атака.

A.K. YATSENKO, V.I. DUBROVIN, L.Y. DEYNEGA
Zaporizhzhia Polytechnic National University

ANALYSIS OF SOFTWARE-DEFINED NETWORK TRAFFIC USING ENTROPY

Software-defined networking (SDN) is an approach to building a network that uses software controllers or application programming interfaces (APIs) to communicate with the underlying hardware infrastructure and route network traffic instead of physical routers and switches.

Software-defined networks use a centralized controller, so ensuring the reliability of its operation is very important for the functioning of the network.

The issue of security becomes especially acute when the number of network users increases. One of the biggest and most common threats to software-defined networks is a distributed denial of service (DDoS) attack.

To detect network attacks, statistical characteristics of network traffic such as the sample mean, sample variance, Pearson's chi-square test, and the information-theoretic measure entropy can be used. Quantitatively, entropy is characterized using the entropy of C. Shannon's probability distribution.

Information entropy is a measure of uncertainty associated with a random variable. Entropy characterizes the probability with which a certain state is established, it is a measure of chaos or irreversibility. The greater the chaos of the system, the higher the value of entropy, and vice versa.

Software complexes are based on entropy analysis of network data recorded by NetFlow sensors. Typical sensors connect to TAP or SPAN ports on switches. Streams are analyzed during fixed time intervals. The collected streams are registered in a database and then analyzed. Anomaly filters are provided by direction, protocol, and subnet. Next, the entropy value of positive and negative values of α for the distribution of motion characteristics is calculated.

In the detection step, the observed entropy is compared with the minimum and maximum values stored in the profile, and an anomaly threshold is determined. Threshold values less than 0 or greater than 1 indicate abnormal concentration or variance, respectively.

One solution to detect such attacks is to use fusion entropy. This method allows you to detect DDoS attacks in a time close to real, and the entropy values for normal and malicious traffic differ by 90%.

Keywords: anomaly detection, entropy, netflow, network traffic measurement, software-defined network, DDoS-attack.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

Постановка проблеми

Одним із найефективніших індикаторів аномальної поведінки мережі є аналіз трафіку в реальному часі. Виявлення аномалій – це виявлення спостережень, які не відповідають очікуваній поведінці. Для цього використовуються різні параметри мережевого трафіку, такі як адреси та порти джерела та призначення, кількість підключень тощо.

Програмно-визначена мережа (software-defined network, SDN) – це підхід до побудови мережі, яка використовує програмні контролери або інтерфейси прикладного програмування (application programming interface, API) для зв'язку з основною апаратною інфраструктурою та маршрутизації мережевого трафіку замість фізичних маршрутизаторів і комутаторів.

Мережі передачі даних є місцем, яке обмежує зростання продуктивності додатків із зростанням кількості користувачів. У мережах SDN завдання комутації трафіку та завдання управління суворо розділені. Контролер виступає джерелом керуючої логіки.

Існує три частини типової архітектури SDN:

- програми, які надають запити ресурсів або інформацію про мережу в цілому;
- контролери, які використовують інформацію з програм, щоб вирішити, як маршрутизувати пакет даних;
- мережеві пристрої, які отримують інформацію від контролера про те, куди були переміщені дані.

Програмно-визначені мережі використовують централізований контролер, тому забезпечення надійності його роботи має дуже важливе значення для функціонування мережі [1].

Питання безпеки стає особливо гострим, коли кількість користувачів мережі зростає. Однією з найбільших і найпоширеніших загроз для програмно-визначених мереж є атака розподіленої відмови в обслуговуванні (distributed denial of service, DDoS).

DDoS-атака – хакерська атака на комп'ютерну систему з метою виведення її з ладу. Це створення таких умов, за яких чесні користувачі не зможуть отримати доступ до системних ресурсів (серверів), або цей доступ буде ускладнений [2]. Він може знищити доступні мережеві служби користувача, серйозно загрожуючи мережі. Коли зловмисники надсилають у мережу шкідливі пакети даних, звичайний трафік не може бути оброблений через споживання мережевих ресурсів. У результаті мережі та сервери блокуються, а звичайні послуги перериваються. SDN часто є мішенню для DDoS-зловмисників через централізований контроль.

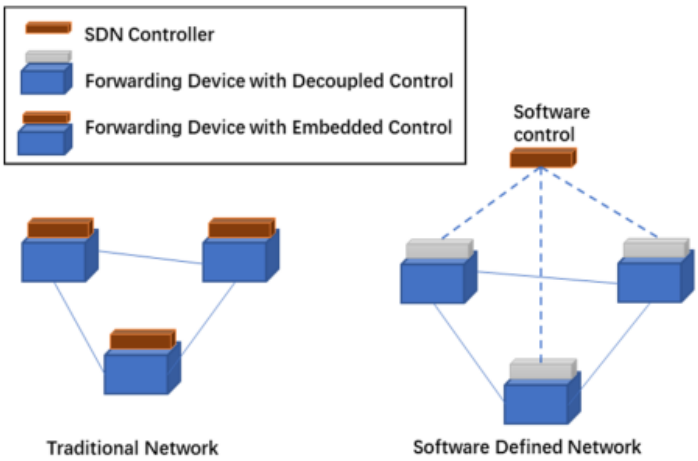

Рис. 1. Відокремлене керування в SDN проти традиційної мережі [3]

Ефективним способом виявлення атак у мережах є аналіз трафіку. Вимірювання параметрів трафіку та їх аналіз допоможе нам вчасно визначити ризик атаки.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

Вивчення аномалій на основі ентропії вивчається для вдосконалення традиційних підходів до аналізу мережевого потоку на основі обсягу та правил.

Аналіз останніх досліджень і публікацій

Характер руху залежить від багатьох факторів, таких як час доби або день тижня. Методи аналізу даних дозволяють за його параметрами виявляти аномальний характер трафіку. Відмінності між нормальним і аномальним інтернет-трафіком протягом дня показано на рис. 2-3

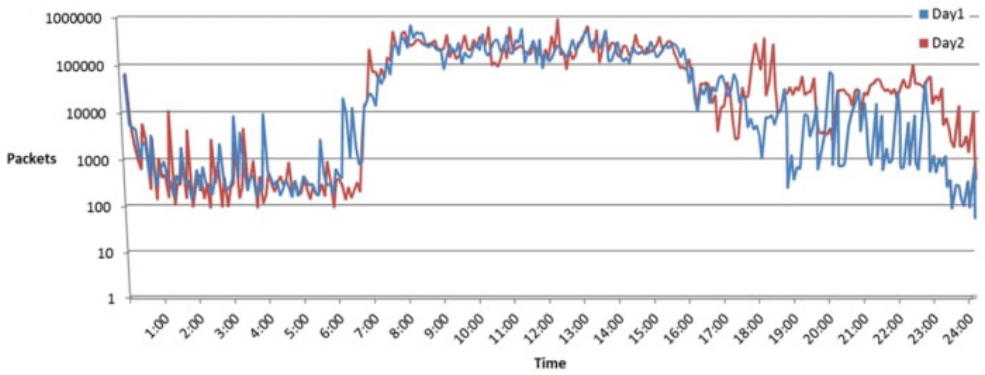

Рис. 2. Профіль нормального трафіку за кількістю пакетів [4]

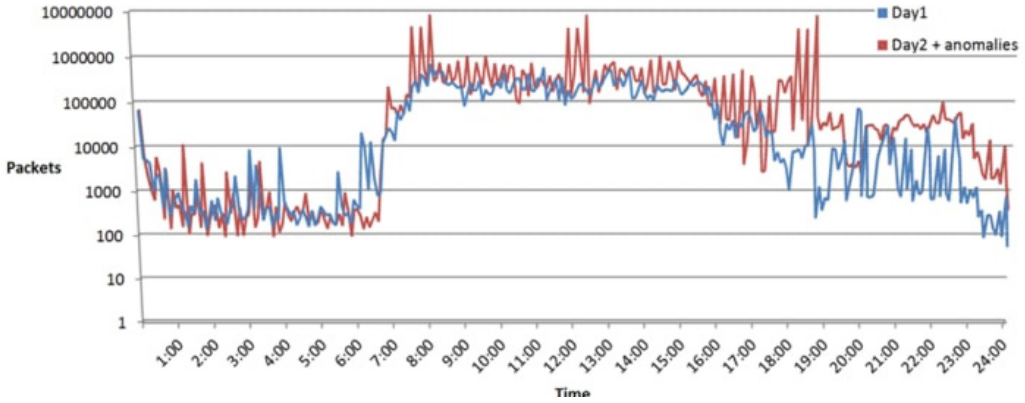

Рис. 3. Легітимний і аномальний трафік за кількістю пакетів [4]

Видно, що атаки видно на профілі трафіку як раптові піки. Однак пошук за атаками вручну неефективний, оскільки це буде повільний процес із високою ймовірністю помилки.

Для аналізу трафіку використовуються різні методи, такі як: вейвлет-аналіз, кластерний аналіз та інформаційна ентропія.

Вейвлет аналіз

Вейвлет-аналіз полягає в побудові коефіцієнтів, які використовуються в розкладі вихідного сигналу за базисними функціями. Сигналом можна вважати інтенсивність мережевого трафіку [5] або дані про співвідношення IP-адрес призначення [6]. Виконання вейвлет-перетворення дозволяє виділити найбільш значущу інформацію як сигнал, що відповідає коливанням з високою амплітудою, і ігнорувати менш корисну інформацію в коливаннях з низькою амплітудою як шумову складову. Концепцію вейвлета ввели Гроссман і Морле (рис. 4).

Вейвлет-перетворення дуже схоже на віконне перетворення Фур'є, але методи використовують інші функції оцінки. Вейвлет-перетворення, на відміну від перетворення Фур'є, не розкладає сигнал на складові у вигляді синусів і косинусів, а використовує особливості, локалізовані як в реальному просторі, так і в просторі Фур'є.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

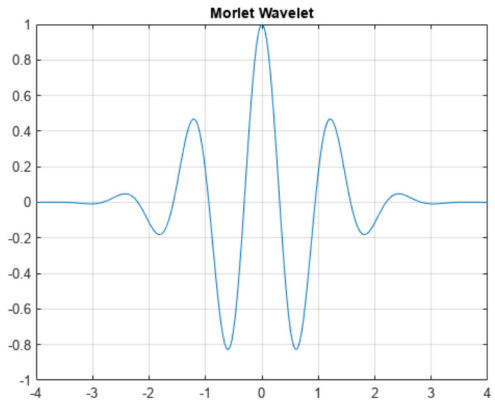

Рис. 4. Вейвлет Морле [7]

Перевага вейвлет-перетворення полягає в тому, що воно покриває фазову площину комірками однакової площі, але різної форми. Це дозволяє нам добре локалізувати низькочастотні деталі сигналу в частотній області (домінуючі гармоніки), а високочастотні деталі в часовій області (раптові стрибки, піки тощо).

Недоліками вейвлет-аналізу є неоднозначність вибору базисних функцій, висока обчислювальна складність при обчисленні коефіцієнтів розкладання сигналу. Крім того, завдання правильного налаштування розміру вікна не є тривіальною. Як зазначено в [8], якщо розмір ковзного вікна набагато більший за тривалість аномалії, то атака буде пропущена, оскільки сплеск частоти, що відповідає тривалості, може бути згладжений. Інакше, якщо розмір вікна занадто малий, то потік безглуздих аномалій неминучий.

Кластерний аналіз

Суть кластерного аналізу полягає у виділенні з мережевого трафіку таких характеристик, які дозволять розділити класифіковані об'єкти (пакети, з'єднання) на групи, що відповідають нормальному функціонуванню мережевої взаємодії. Усі інші екземпляри, які не потрапляють у сконструйовані ділянки, класифікуються як аномальні [9].

Розрізняють ієрархічні (агломераційний і розділовий) та неієрархічні (метод k-середніх, двоетапний кластерний аналіз, метод найближчого сусіда) методи кластерного аналізу. Однак загальноприйнятої класифікації методів кластерного аналізу не існує, і вони включають багато алгоритмів машинного навчання, які вирішують проблему поділу сукупності на однорідні групи (рис. 5).

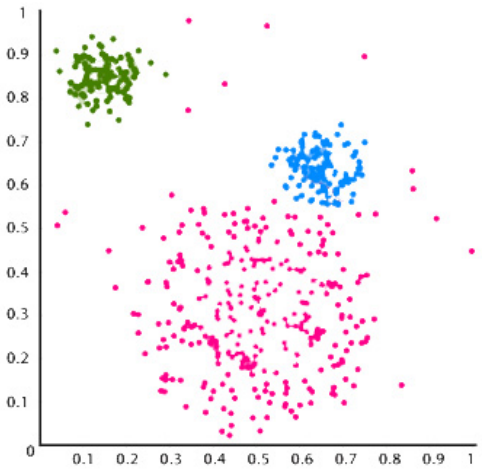

Рис. 5. Приклад кластерів

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

Великою перевагою кластерного аналізу є те, що він дозволяє розбивати об’єкти не за одним параметром, а за цілим набором ознак. Крім того, кластерний аналіз, на відміну від більшості математичних і статистичних методів, не накладає жодних обмежень на тип об'єктів, що розглядаються, і дозволяє розглядати набір вихідних даних практично довільного характеру. Кластерний аналіз дозволяє розглядати досить великий обсяг інформації і різко скорочувати великі обсяги інформації, роблячи їх компактними і наочними.

Основними недоліками кластерного аналізу є упереджені вибірки та високі помилки вибірки. Якщо кластери, що представляють всю сукупність, були сформовані на основі упередженої думки, висновки щодо всієї сукупності також будуть упередженими.

Інформаційна ентропія

Ентропійний аналіз використовується при виявленні атак для формування статистичного критерію, щоб перевірити, чи належить досліджуваний екземпляр до класу відхилень [10].

Основна ідея методу полягає в побудові моделі, яка б максимізувала значення ентропії. Це відповідає припущенню, що зі збільшенням кількості унікальних записів вони рівномірно розподіляються відносно обраних класів множини, що призводить до зростання ентропії.

Щоб виявити аномалії, автори [11] спочатку застосовують метод максимальної ентропії для створення нормальної моделі, в якій обрані класи мережевих пакетів мають найкращий рівномірний розподіл. Потім умовна ентропія використовується для виявлення відмінностей між розподілом класів пакетів у поточному трафіку порівняно з розподілом, отриманим за допомогою методу максимальної ентропії.

Основна перевага ентропії полягає в тому, що вона дозволяє встановлювати різні ваги для атрибутів, визначаючи важливість кожного параметра для поточного завдання. Її вважають придатним для всіх процесів прийняття рішень, що вимагають визначення ваги. Ентропія може забезпечити кількісну міру вмісту інформації, яка може порівнювати та аналізувати ефект використання різних статистичних моделей, алгоритмів і пов’язаних налаштувань: що нижча ентропія критерію, то більш цінну інформацію містить критерій. Метод вимірює невизначеність змінних і оцінює вплив основних факторів на результат.

Основним недоліком методу оцінки ентропійної ваги була висока чутливість значущості до значень ентропії різних критеріїв. Але значення ентропії показали вищу чутливість для оцінки ваги до наборів даних вищої розмірності, ніж до менших розмірів [12].

В результаті аналізу було вирішено використовувати інформаційну ентропію для аналізу трафіку.

Мета дослідження

Основна мета дослідження – довести, що підхід, заснований на ентропії, підходить для виявлення сучасних шкідливих програм, схожих на ботнет, на основі аномальних мережевих шаблонів.

Щоб виявити атаки у мережі, ви можете використовувати її статистичні характеристики як параметри мережевого трафіку, такі як середнє значення вибірки, дисперсія вибірки, критерій хі-квадрат Пірсона та теоретико-інформаційна міра – ентропія. Кількісно ентропія характеризується за допомогою ентропії розподілу ймовірностей К. Шеннона.

Мета полягає в тому, щоб підвищити ефективність систем виявлення вторгнень, систем виявлення аномалій і систем управління інформаційною безпекою, провести теоретичні та експериментальні дослідження щодо можливості використання обчислених у реальному часі значень інформаційної ентропії як базової атаки і індикатор мережевих послуг.

Інформаційна ентропія – це міра невизначеності, пов'язана з випадковою величиною. Ентропія характеризує ймовірність P, з якою встановлюється той чи інший стан, є мірою хаотичності чи незворотності [13]. Чим більша хаотичність системи, тим вище значення ентропії, і навпаки.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

$$H_S(X) = \sum_{i=1}^{n} p(x_i) \log_a \frac{1}{p(x_i)} \quad (1)$$

де X – знак, який може приймати значення $\{ x_1, ..., x_n \}$,
$p(x_i)$ – функція ймовірності результату x_i,
n – кількість можливих станів.

З метою виявлення аномалій зазвичай використовуються вибіркові ймовірності, оцінені кількістю випадків x і у часовому вікні t. Значення ентропії залежить від випадковості (вона досягає максимуму, коли ймовірність $p(x_i)$ однакова для всіх x_i), а також від значення n. Щоб вимірювати лише випадковість, слід застосовувати нормалізовані форми.

Викладення основного матеріалу дослідження

Для цієї роботи було розроблено програмне забезпечення для розрахунку ентропії. В якості вихідних даних для тестування програмного забезпечення були взяті значення параметрів моделювання DDoS-атаки, отримані при розробці методики ентропійних досліджень Бабенко Т. В. [14]. Їх можна побачити в таблиці 1.

Таблиця 1

Параметри моделювання DDoS-атаки

№ послідовності	Розмір послідовності (пакету)	Тривалість збору пакетів	
		Нормальний режим	Режим моделювання атаки
1	50 000	15	2
2	100 000	30	3
3	150 000	60	5

Кількість пакетів за секунду є найбільш очевидним показником наявності або відсутності DDoS-атаки. Ці параметри дозволяють аналізувати трафік за часом збору певної кількості пакетів (50000, 100000, 150000). Для експерименту також додали опцію, що 50 000 пакунків збирають за 145 хвилин. Незважаючи на те, що це не атака, визнання такої події аномальною дозволить завчасно виявити проблеми в мережі (наприклад, збій обладнання).

Окрім кількості пакетів за секунду, аналізувалися IP-адреси джерела та призначення. Імовірність атаки є високою в таких випадках: або аномально багато пакетів надходять з однієї адреси (DoS), або аномально багато запитів надходять на одну адресу (DDoS). Аналіз декількох параметрів підвищить точність виявлення.

За цими параметрами розраховується значення ентропії. Після цього значення порівнюється зі звичайним профілем трафіку шляхом розрахунку порогу аномалії. Значення різних параметрів (пакетів за секунду, адрес джерела та призначення) аналізуються разом і визначається остаточна ймовірність атаки.

Архітектура кінцевого програмного комплексу наведена на рис. 6.

Рис. 6. Схема програмного комплексу

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

Кінцевий програмний комплекс збиратиме дані, зареєстровані датчиками NetFlow. Типові датчики, такі як маршрутизатори або спеціальні датчики (наприклад, Softlowd), будуть підключені до портів TAP або SPAN на комутаторах. Потоки будуть аналізуватися протягом фіксованих інтервалів часу (кожні 5 хвилин). Зібрані теми будуть зареєстровані в базі даних. Після цього до зібраних даних будуть застосовані фільтри вибору функцій, щоб отримати необхідні характеристики (пакети за секунду, адреси джерела та призначення тощо). Потім для кожного параметра обчислюються значення ентропії. На етапі нормалізації значення порогу обчислюється за допомогою звичайного профілю трафіку. Після обчислення порогових значень можна класифікувати випадок і визначити, чи характер трафіку є зловмисним чи ні.

Розроблене програмне забезпечення має виявляти аномальну поведінку мережі за розрахованим пороговим значенням. Для послідовностей 1-3 у режимі моделювання атаки значення мають бути від'ємними, тоді як для послідовності 4 у режимі атаки вони мають бути більшими за 1. Для нормального режиму поріг має бути в діапазоні від 0 до 1.

Результати розрахунку порогу наведені в таблиці 2.

Таблиця 2

Результати класифікації

№ послідовності	Розмір послідовності (пакету)	Розрахований поріг	
		Нормальний режим	Режим моделювання атаки
1	50 000	0,08	-0,18
2	100 000	0,4	-0,15
3	150 000	0,96	-0,08
4	50 000	0,96	1,12

Видно, що значення порогу чітко вказує на наявність аномалії – значення менше 0 для аномальної концентрації та значення більше 1 для аномальної дисперсії. Це підтверджує ефективність запропонованого методу виявлення атак.

Розраховані пороги можуть бути використані в подальшому аналізі всього трафіку. Врахування кількох параметрів допоможе зробити аналіз більш точним і виявити джерела проблем.

Висновки

Завдання розробки програмного забезпечення для виявлення шкідливого трафіку є надзвичайно важливим як для звичайних, так і для програмно-визначених мереж. Крім того, питання безпеки та захисту в програмно-визначених мережах є надзвичайно важливим, оскільки управління централізовано в контролері SDN, що робить його вразливим до атак. Аналіз на основі ентропії дозволяє виявити загрози на ранній стадії та вчасно усунути джерело проблеми.

У цій статті розглядаються можливості використання ентропії для аналізу трафіку програмно визначеної мережі. Ентропійний аналіз є потужним інструментом у боротьбі з мережевими загрозами, такими як DDoS-атаки.

Ентропійний аналіз був розроблений для виявлення аномальної поведінки мережі. Кількість пакетів за секунду, IP-адреси джерела та призначення пакетів використовувалися як вхідні значення для аналізу, оскільки вони є найбільш яскравими індикаторами наявності чи відсутності атаки. Результат обчислення ентропії порівнюється зі звичайним профілем трафіку.

У роботі запропоновано архітектуру програмного комплексу. Таке програмне забезпечення дозволить підвищити безпеку в програмно-визначених мережах і знизити вразливість контролера SDN до DDoS-атак.

Надалі планується вдосконалити роботу програмного комплексу. До аналізу планується додати більше параметрів, таких як середня тривалість потоку, кількість вхідних і вихідних з'єднань на хост.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

Крім того, планується розробити алгоритм оцінки набору отриманих значень. Такий алгоритм враховуватиме ваги параметрів, тому найбільш очевидний показник атаки матиме найбільший вплив на вихід результату.

Список використаної літератури

1. G What is Software-Defined Networking (SDN)? [Електронний ресурс]. – Режим доступу: https://www.vmware.com/topics/glossary/content/software-defined-networking.html
2. DoS атака [Електронний ресурс]. – Режим доступу: uk.wikipedia.org/wiki/DoS attack
3. Fan C., Kaliyamurthy N.M., Che S., Jiang H., Zho Y. and Campbell C. Detection of DDoS Attacks in Software Defined Networking Using Entropy. 2022, 12, 370.
4. Bereziński P., Jasiul B. and Szpyrka M. An entropy-based network anomaly detection method, *Entropy*. 2015, 17(4). P. 2367-2408.
5. Barford P., Plonka D. Characteristics of Network Traffic Flow Anomalies. *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*. 2001. P. 69–73.
6. Kim S.S., Reddy A.L. Statistical techniques for detecting traffic anomalies through packet header data. *IEEE/ACM TON*. 2008. V. 16. Issue 3. P. 562–575.
7. Morlet wavelet [Електронний ресурс]. – Режим доступу: https://www.mathworks.com/help/wavelet/ref/morlet.html
8. Barford P., Kline J., Plonka D., Ron A. A signal analysis of network traffic anomalies. *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement*. 2002. P. 71–82.
9. Lee K., Kim J., Kwon K.H., Han Y., Kim S. DDoS attack detection method using cluster analysis. *Expert Systems with Applications*. 2008. V. 34. Issue 3. P. 1659–1665.
10. Branitskiy A., Kotenko I. Analysis and Classification of Methods for Network Attack Detection. *SPIIRAS Proceedings*, 2016, 2(45):207.
11. Gu Y., McCallum A., Towsley D. Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation. *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*. 2005. P. 32–32.
12. Robert M.X. Wu, Yongwen Wang. Which Objective Weight Method Is Better: PCA or Entropy?. *Scientific Journal of Research and Reviews*, 2022.
13. Shannon C. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* 1948, 27, 379–423.
14. Бабенко Т. В. Дослідження ентропії мережевого трафіка як індикатора DDOS-атак. *Науковий вісник Національного гірничого університету*. 2013. № 2. С. 86-89.

References

1. G What is Software-Defined Networking (SDN)? [Electronic resource]. – Access mode: https://www.vmware.com/topics/glossary/content/software-defined-networking.html
2. DoS attack [Electronic resource]. – Access mode: uk.wikipedia.org/wiki/DoS attack
3. Fan, C., Kaliyamurthy, N.M., Che, S., Jiang, H., Zho, Y. & Campbell, C. (2022). Detection of DDoS Attacks in Software Defined Networking Using Entropy. **12**, 370.
4. Bereziński, P., Jasiul, B., & Szpyrka, M. (2015). An entropy-based network anomaly detection method, *Entropy*. **17**(4), 2367-2408.
5. Barford, P., & Plonka, D. (2001). Characteristics of Network Traffic Flow Anomalies. *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*. 69–73.
6. Kim, S.S., & Reddy, A.L. (2008). Statistical techniques for detecting traffic anomalies through packet header data. *IEEE/ACM TON*. **16** (3), 562–575.
7. Morlet wavelet [Electronic resource]. – Access mode: https://www.mathworks.com/help/wavelet/ref/morlet.html
8. Barford, P., Kline, J., Plonka, D., & Ron, A. (2002). A signal analysis of network traffic anomalies. *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement*. 71–82.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14

9. Lee, K., Kim, J., Kwon, K.H., Han, Y., & Kim, S. (2008). DDoS attack detection method using cluster analysis. *Expert Systems with Applications*. **34** (3), 1659–1665.
10. Branitskiy, A., & Kotenko, I. (2016). Analysis and Classification of Methods for Network Attack Detection. *SPIIRAS Proceedings*. **2** (45):207.
11. Gu, Y., McCallum, A., & Towsley, D. (2005). Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation. *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*. 32–32.
12. Robert, M.X. Wu, Yongwen, Wang. (2022). Which Objective Weight Method Is Better: PCA or Entropy?. *Scientific Journal of Research and Reviews*.
13. Shannon, C. (1948). A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **27**, 379–423.
14. Babenko, T. V. (2013). Research on the entropy of tethered traffic as an indicator of DDOS attacks. *Science Bulletin of the National Grooming University*. **2**, 86-89.

Яценко Анастасія Костянтинівна – студентка кафедри програмних засобів Національного університету «Запорізька політехніка». E-mail: nastya.yatsenko.zp@gmail.com, ORCID: 0000-0002-5675-5205.

Дубровін Валерій Іванович – професор кафедри програмних засобів Національного університету «Запорізька політехніка». E-mail: vdubrovin@gmail.com, ORCID: 0000-0002-0848-8202.

Дейнега Лариса Юріївна – старший викладач кафедри програмних засобів Національного університету «Запорізька політехніка». E-mail: deynega.larisa@gmail.com, ORCID: 0000-0003-0304-4327.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-14