

УДК 004.056.57

Дубровін В.І.¹, Дейнега Л.Ю.², Горпініч І.О.³

¹ проф. НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

³ студ. гр. КНТ-131 НУ «Запорізька політехніка»

ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДА ВИЯВЛЕННЯ АТАК У МЕРЕЖАХ ЗА ДОПОМОГОЮ ЕНТРОПІЇ

В сучасних мережах питання виявлення атак є критично важливим через постійне зростання обсягів трафіку та складності атак. Класичні методи виявлення аномалій часто не справляються зі швидкими змінами в поведінці трафіку або недостатньо ефективні для обробки великих обсягів даних. Одним із перспективних підходів є використання ентропії для аналізу трафіку [1 - 3]. Ентропія дозволяє виявляти відхилення від нормального функціонування системи, оскільки під час атак статистичні характеристики трафіку змінюються. Завдання цієї роботи полягає у дослідженні методів виявлення аномалій у мережевому трафіку за допомогою ентропії для виявлення потенційних атак [4 - 5].

В даному дослідженні проведено аналіз мережевого трафіку [6], зібраного з файлу формату PCAP, за допомогою бібліотек `scapy` та `matplotlib`. Основною метою дослідження було визначення ентропії джерел і призначених IP-адрес, а також портів, що використовуються в пакетах даних. Ентропія, яка вимірює невизначеність у даних, обчислюється шляхом підрахунку частот виникнення кожного унікального значення в масивах IP-адрес і портів. Результати представлено у вигляді гістограм, що ілюструють розподіл джерел IP, призначених IP і портів.

Результати проведеного дослідження представлено на рис.1.



Рисунок 1 – результат роботи програми

Ентропія джерел IP: 1.451 - це значення вказує на ступінь випадковості або невизначеності серед IP-адрес, які є джерелами трафіку. Чим більше ентропія тим більше унікальних джерел IP і більш рівномірно розподілений трафік між ними. Значення 1.451 свідчить про те, що є кілька різних джерел IP, але це не дуже висока ентропія, що може вказувати на переважання кількох основних джерел у потоці трафіку.

Ентропія призначених IP: 1.429 - це значення показує ступінь невизначеності для IP-адрес, на які спрямовується трафік. Подібне значення (1.429) до ентропії джерел IP свідчить, що розподіл призначених IP є схожим на розподіл джерел IP. Тобто, кількість призначених IP є також обмеженою, і основна частина трафіку спрямовується до кількох вузлів.

Ентропія портів: 2.155 - це значення вказує на ступінь невизначеності серед портів, через які проходить трафік. Значення 2.155 є вищим, ніж для IP-адрес, що може свідчити про більшу різноманітність портів, через які передаються дані. Це може бути ознакою того, що використовується широкий спектр портів для комунікації, що є типовим для мереж із різними сервісами або протоколами.

Графіки, які були отримані в результаті роботи програми показано на рис.2 – 4.



Рисунок 2 – Графік 1



Рисунок 3 – Графік 2

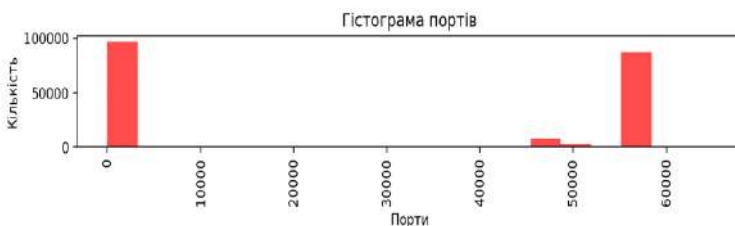


Рисунок 4 – Графік 3

Графік 1 показує розподіл IP-адрес джерел трафіку. Більшість трафіку надходить із однієї або кількох IP-адрес, що вказує на домінуючі джерела й можливу централізацію або аномалію, пов'язану з атакою. Також спостерігається мала кількість унікальних IP-джерел, що може бути нормальним для локальних мереж, але також свідчити про значне навантаження на одне або кілька джерел.

Графік 2 вказує на домінування трафіку, спрямованого до однієї IP-адреси (192.168.202.79), що може свідчити про централізований сервер або атаку типу DDoS. Невелика кількість унікальних IP-адрес вказує на обмежену взаємодію між пристроями мережі.

Графік 3 показує домінування трафіку на низьких портах (0-10000), що свідчить про використання стандартних сервісів, а також інтенсивний трафік на високих портах (близько 60000), що може вказувати на короткочасні з'єднання чи нестандартні сервіси

Аналіз мережевого трафіку за допомогою ентропії дозволяє виявляти аномалії та оцінювати різноманітність даних, таких як IP-адреси та порти. Високі значення ентропії вказують на більшу різноманітність трафіку, що може свідчити про нормальну активність, тоді як низькі значення можуть бути ознакою потенційних загроз або нестандартної поведінки. Використання гістограм для візуалізації результатів допомагає краще зрозуміти структуру мережевих даних та зробити висновки щодо стану мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дубровин В. И. Исследование изменений энтропии и энергии на этапах декомпозиции сигнала / Дубровин В. И., Твердохлеб Ю. В. // Радиоэлектроника, информатика, управление. – 2013. – No2 (29). – С. 54–58.
2. Дубровін В.І. Аналіз мережевого трафіку за допомогою ентропії / А. К. Яценко, В. І. Дубровін, Ю.В. Твердохліб // Матеріали XXIII Міжнародного науково-практичного семінару імені А.Я. Петренюка. – Запоріжжя – Кропивницький: ПП Ексклюзив-Систем, 2021. – С. 198-202.

3. Detection and Mitigation of DDoS Attacks Using Conditional Entropy in Software-defined Networking Ming Xuanyuan; Visham Ramsurrun; Amar Seeam (2019) - <https://ieeexplore.ieee.org/document/9087252>

4. A Review of Detecting DDoS Attacks Based on Entropy Computation Atul Agrawal, Pashupati Baniya, Bishnu Bahadur Gupta (2023) - https://www.researchgate.net/publication/378323236_A_Review_of_Detecting_DDoS_Attacks_Based_on_Entropy_Computation

5. SDN Based DDoS Mitigating Approach Using Traffic Entropy for IoT Network Muhammad Ibrahim, Muhammad Hanif Anjum, Shabir Ahmad (2024)https://www.researchgate.net/publication/379783029_SDN_Based_DDos_Mitigating_Approach_Using_Traffic_Entropy_for_IoT_Network

6. Посилання на джерело з файлом мережевого трафіку: <https://share.netresec.com/s/7qgDSGNGw2NY8ea>.