Раздел 5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ДОСЛІДЖЕННЯ ЕНТРОПІЇ МЕРЕЖЕВОГО ТРАФІКУ МЕТОДОМ ЧАСОВОГО ВІКНА

Т.В. Бабенко, С.О. Сушко, В.П. Мойсєєнко
(Україна, Дніпропетровськ, ДВНЗ «Національний гірничий університет»)

Одна з останніх тенденційу сфері комп'ютерних злочинів – зростання кількості і складності атак на доступність інформації. Такі вторгнення утворюють клас атак «відмова в обслуговуванні» (DoS-атаки). Коли ж вторгнення здійснюється з великої кількості пристроїв з метою блокування або виведення з ладу інтернет-сервісів та ресурсів, то її відносять до атак типу DDoS – розподілена відмова в обслуговуванні. Останнім часом кількість таких атак зросла багаторазово і на сьогодні має максимальну частку від загальноїкількості атак. Актуальною проблемою стає розпізнавання атаки на початкових етапах для прийняття необхідних заходів та забезпечення доступності ресурсу.

Існуючі методики виявлення мережевих аномалій щодо принципу їх дії зазвичай розділяють на два види: сигнатурний і поведінковий. Але обидва методи повністю не виявляють аномальну активність трафіку, що частково пов’язано з недостатністю теоретичних досліджень. У 1994 р. В. Леланд виявив, що в умовах DDOS-атак агрегований мережевий трафік стає персистентним та самоподібним [1]. У 2003 р. Файнштейн і Шнахенберг [2] показали, що як індикатор атак можна розглядати такі статистичні характеристики мережевого потоку, як вибіркове середнє, вибіркову дисперсію та критерій згоди Пірсона χ^2 або інформаційно-теоретичну міру – ентропію IP-атрибутів. Вивчення окремих аспектів даної теми, зокрема використання ентропії Шеннона для аналізу аномалій мережевого трафіка, наведено у [3,4].

У даній роботі основним індикатором для виявлення мережевих аномалій вибрана ентропія Шеннона. Тому аномалія трафіку трактується нами як подія, що супроводжується відхиленням від стандартних значеньентропії, отриманих на основі раніше зібраних нормальних профілів поводження системи.

Для дослідження мережевий трафік було структуровано. Вхідний мережевий пакет розглядався як множина параметрів «вхідний порт(PORT_D)», «IP-адреса відправника(IP_S)» та «час надходження(COME_TIME)». Схема структуризації мережевого трафіку показана на рис.1.

Запис мережевого трафіку у наведеному форматі здійснено за допомогою спеціально розробленого програмного забезпечення на основі відкритих бібліотек WinPCap, jpcap. Для аналізу сформовано послідовності з 20000, 35000, 50000, 75000 та 100000 пакетів.

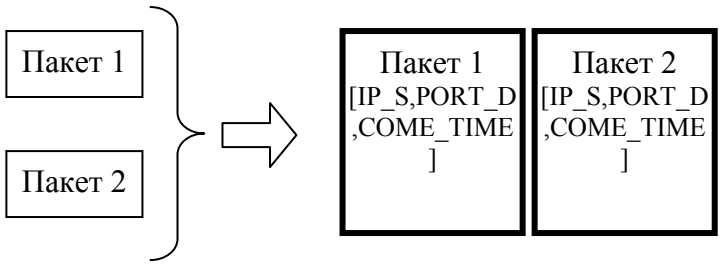

Рис. 1. Структуризація мережевих пакетів

За формулою Шеннона [5] ентропія трафіка залежіть від ймовірностей p_i появи пакетів при їх передачі:

$$H(x) = -\sum_{i=1}^{n} p_i \cdot \log_2 p_i , \qquad (1)$$

де в якості ймовірності появи p_i пакету i-го типу може виступати його частота $f_i = \frac{n_i}{N}$, n_i – кількість пакетів i-го типу, N – загальна кількість пакетів трафіку.

Аналіз мережевого трафіку проводився за допомогою методу часового вікна, за яким часова вісь розбивається на «вікна» фіксованого розміру (часові інтервали) і за допомогою параметру COME_TIME пакету з'ясовується, чи потрапив він у вікно. Далі фіксується загальна кількість пакетів у вікні та обчислюється ентропія за формулою (1). Схема методу часового вікна представлена на рис. 2.

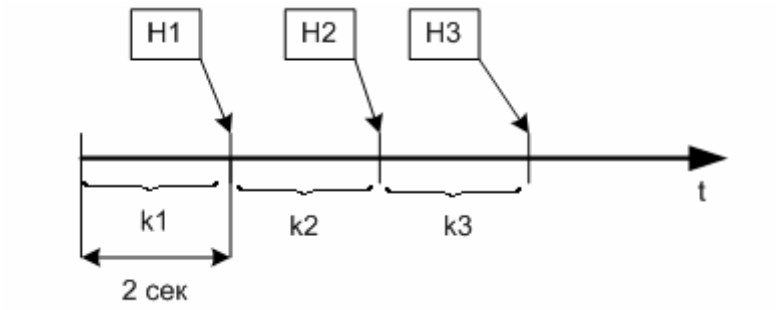

Рис. 2. Схема методу часового вікна: H – значення ентопії Шенона, обчислене для пакетів у вікні, k – кількість пакетів, що потрапила у вікно

Метод дає змогу проводити аналіз мережевого трафіку у режемі, наближенному до режиму реального часу, а також зменшує навантаження на обчислювальну систему. Зрозуміло, що збільшення розмірів вікна зменшує чутливість методу. За нашими розрахунками найбільш оптимальним є вікно розміром 2 с.

Для аналізу використовувалися дані, зібрані за «чистий» період, коли мережа функціонувала у нормальному штатному режимі, і дані, зібрані за

аномальний період при наявності мережевої атаки. Емуляція підвищеної мережевої активності проводилася шляхом додавання до досліджувальної послідовності пакетів трафіку, що є близьким до використовуваного при атаках DDoS.

В якості кінцевої характеристики послідовності використовується зважена сума ентропії Шенона, що обчислюється за формулою:

$$W = \frac{\sum_{i=1}^{n}(H_i k_i)}{\sum_{i=1}^{n} k_i}$$

Результати досліджень представлені в таблиці 1.

Таблиця 1

Результати дослідження

№ п\п	Розмір послідовності (пакети)	Додано пакетів	Зважена ентропія без атаки (біт)	Зважена ентропія з атакою (біт)
1	20 000	2000	1,9534	1,5475
2	35 000	3500	1,9312	1,4593
3	50 000	5000	1,7634	1,0848
4	70 000	7000	1,8534	1,2473
5	100 000	10000	1,8456	1,1874

З таблиці 1 видно, що зважена ентропія послідовності пакетів без атаки вища, ніж ентропія послідовності при наявності атаки.

Для відстеження процесу в динаміці були побудовані графікизалежності кількості пакетів у вікні (рис.3) та залежності ентропії від часу (рис. 4). На рис.3 на відрізку [49 с; 170 с] видна суттєва різниця у кількості пакетів, що потрапляють у вікно між послідовністю без атаки (пунктирна лінія) та послідовністю з атакою (крапки). На тому ж часовому відрізку на графіку зміни ентропії спостерігається падіння ентропії при атаці порівняно з ентропією трафіку у не аномальному стані.

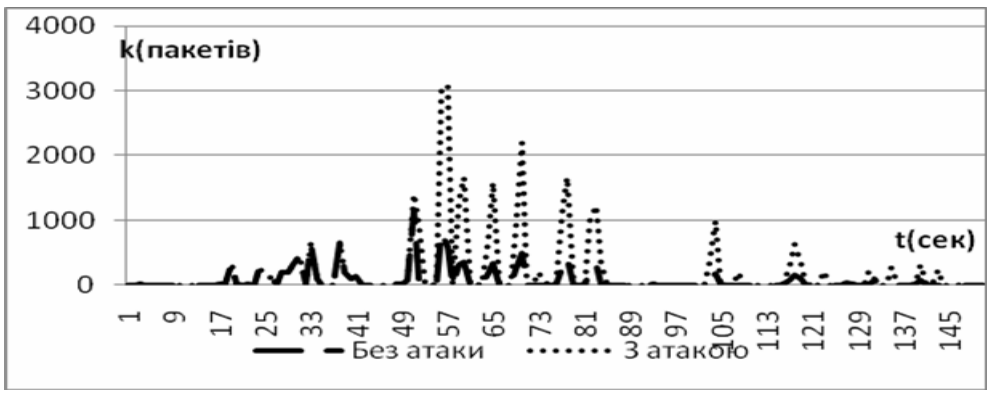

Рис. 3 Графік зміни кількості пакетів у вікні

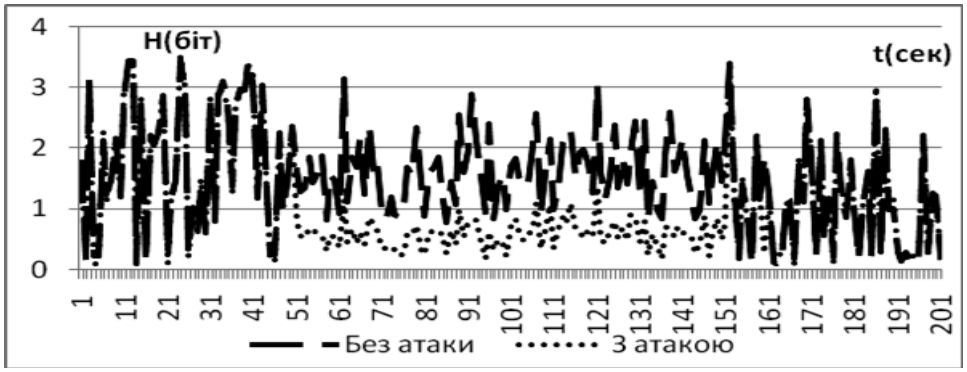

Рис. 4. Графік зміни значень ентропії

Таким чином, обчислення ентропії трафіку методом часового вікна та моніторинг кількості пакетів у часовому вікні можна використовувати для аналізу мережевої активності у режимі, наближенному до режиму реального часу,з метою виявлення мережевих аномалій.

Список літератури

1. Leland W.E., Taqqu M.S., Willenger W., Wilson D.V. On the Self-Similar Nature of Ethernet Traffic.IEEE Transactions on Networking, 1994, v. 2, Feb. p.1 – 15.

2. Feinstein L., Schnackenberg D. Statistical Approaches to DDoS Attack Detection and Response. Proceedingsof the DARPA Information Survivability Conference and Expostion (DISCEX'03), April 2003.

3. Борисов Д.Н. Энтропия как индикатор возникновения аномалий сетевого трафика. НауковіпраціДонНТУ, 2007, випуск 118, с. 43 – 49.

4. W.Lee, D.Xiang. Information-Theoretic Measures for Anomaly Detection.Conference: IEEE Symposium on Security and Privacy. – 2001, 130 – 143 p.

5. Шеннон К. Работы по теории информации и кибернетике. М.: Иностранная литература, 1963. – 830 с.

РИСКИ, СВЯЗАННЫЕ С ПЕРЕНОСОМ РЕСУРСОВ В ВИРТУАЛЬНУЮ ИНФРАСТРУКТУРУ

О.Г. Горяная
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Одна из основных характеристик виртуальной среды – динамичность – является как преимуществом для эксплуатирующих служб, позволяющим быстро выполнять операции развертывания и миграции виртуальных машин, так и недостатком для служб информационной безопасности, поскольку именно с этим связаны основные риски в виртуальной среде.

Перенеся производственные серверы на виртуальную платформу, нам следует осознать, что:

– ОС, приложения и данные больше не привязаны к одной физической платформе. Нельзя точно сказать на каком именно сервере работает то или иное приложение.