ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМНИЙ АНАЛІЗ ТА КЕРУВАННЯ

УДК 004.056

Т.В. Бабенко, д-р техн. наук, проф.

Державний вищий навчальний заклад „Національний гірничий університет“, м. Дніпропетровськ, Україна, e-mail: Babenko@nmu.org.ua

ДОСЛІДЖЕННЯ ЕНТРОПІЇ МЕРЕЖЕВОГО ТРАФІКА ЯК ІНДИКАТОРА DDOS-АТАК

T.V. Babenko, Dr. Sci. (Tech.), Professor

State Higher Educational Institution “National Mining University”, Dnipropetrovsk, Ukraine, e-mail: Babenko@nmu.org.ua

RESEARCH OF NETWORK TRAFFIC ENTROPY AS A DDOS-ATTACK INDICATOR

Мета. З метою підвищення ефективності IDS (intrusion detection systems), ADS (anomaly detection system) та систем управління інформаційною безпекою виконати теоретичні та експериментальні дослідження з вивчення можливості використання значень обчисленої в режимі реального часу інформаційної ентропії в якості базового індикатора атаки на мережеві сервіси.

Методика. Методика роботи включає збір статистичної інформації про роботу IP-мережі в нормальному режимі, моделювання процесів, що викликають аномальні стани IP-мережі, збір статистичної інформації про роботу мережі при наявності DDOS-атак на мережеві сервіси, визначення оптимальних розмірів рухомого вікна, обчислення значень інформаційної ентропії та їх порівняння з еталонними для даної IP-мережі.

Результати. Обчислені в реальному масштабі часу значення інформаційної ентропії з використанням методу рухомого вікна є ефективним індикатором аномального стану IP-мережі та можуть бути використані в системах виявлення вторгнень, системах управління інформаційною безпекою.

Наукова новизна. Запропоновано алгоритм обчислення інформаційної ентропії, який на відміну від класичного алгоритму, за рахунок використання методу рухомого вікна дозволяє значно пришвидшити обчислення та виконувати їх в реальному масштабі часу.

Практична значимість. На основі проведених теоретичних та експеременталних досліджень запропоновано методику обчислень інформаційної ентропії, що дозволяє використовувати цей показник для аналізу мережевого трафіку в реальному масштабі часу в IDS, MDS ADS системах.

Ключові слова: *інформаційна ентропія, системи виявлення вторгнення, системи виявлення аномалій, аномальний стан IP-мережі, мережевий трафік, відмови в обслуговуванні, моделювання, захист інформації, безпека інформації*

Постановка проблеми. Інформаційно-комунікаційні системи охоплюють більшість сфер людської діяльності. При цьому навіть самі надійні системи не забезпечують необхідного рівня захисту від мережевих атак на державні та комерційні інформаційні ресурси. Однією з причин цього є те, що, у більшості систем, для виявлення вторгнень IDS (intrusion detection system) [1], зловмисних дій MDC (misuse detection system) та виявлення аномалій ADC (anomaly detection system) використовуються відхилення в роботі систем по відношенню до норми.

Концепція виявлення мережевих вторгнень була вперше запропонована в технічному звіті Дж. Андерсена [2] та розвинута Денінгом у роботі “An intrusion detection model”. Особливу увагу Денінг приділив розробці профілів нормальної активності систем, статистичному аналізу даних, технікам ідентифікації мережевих атак, а також перспективним напрямам розвитку систем виявлення вторгнень.

Як відомо, одним із найбільш ефективних індикаторів аномального поводження мережі є інформаційний аналіз її трафіку в реальному масштабі часу.

Для реалізації такого аналізу використовуються різноманітні параметри мережевого трафіку, які прийнято, як правило, розподіляти на три групи: внутрі-

шні параметри (дані, що отримані із заголовків пакетів); параметри вмісту (показники кількості сеансів суперкористувача, спроб авторизації, створення файлів); параметри трафіку (кількість з'єднань до одного порту та ін.). Параметри, що використовуються при аналізі, повинні дозволяти з високою точністю відрізняти нормальний трафік мережі від аномального.

Для виявлення мережевих аномалій на основі статистичних методів, як правило, використовуються наступні підходи: алгоритми кластеризації (з яких найбільш популярним є метод К-середніх); марковські моделі; вейвлет-аналіз, нейронні мережі, штучні імунні системи.

В якості параметрів мережевого трафіку, для виявлення мережевих атак, також можна використовувати такі його статистичні характеристики як вибіркове середнє, вибіркову дисперсію, критерій згоди Пірсона χ^2 , інформаційно-теоретичну міру – ентропію. Кількісно ентропію характеризують за допомогою ентропії розподілу ймовірностей К. Шеннона.

Метою є підвищення ефективності IDS (intrusion detection systems), ADS (anomaly detection system) та систем управління інформаційною безпекою, виконання теоретичних та експериментальних досліджень із вивчення можливості використання значень обчисленої в режимі реального часу інформаційної ентропії в якості базового індикатора атаки на мережеві сервіси.

Основний матеріал дослідження. У цьому дослідженні вивчення процесів аномального поводження IP-мереж та інформаційний аналіз трафіку в реальному масштабі часу виконували на прикладі моделювання DDoS-атак.

Як відомо, під час DDoS-атаки пакети надсилаються з багатьох джерел, як правило, на один вхідний порт, тому в якості параметрів для аналізу використовували IP-адресу джерела пакета (IP_S) та порт призначення (PORT_D). Принцип структуризації мережевих пакетів графічно представлено на рис. 1.

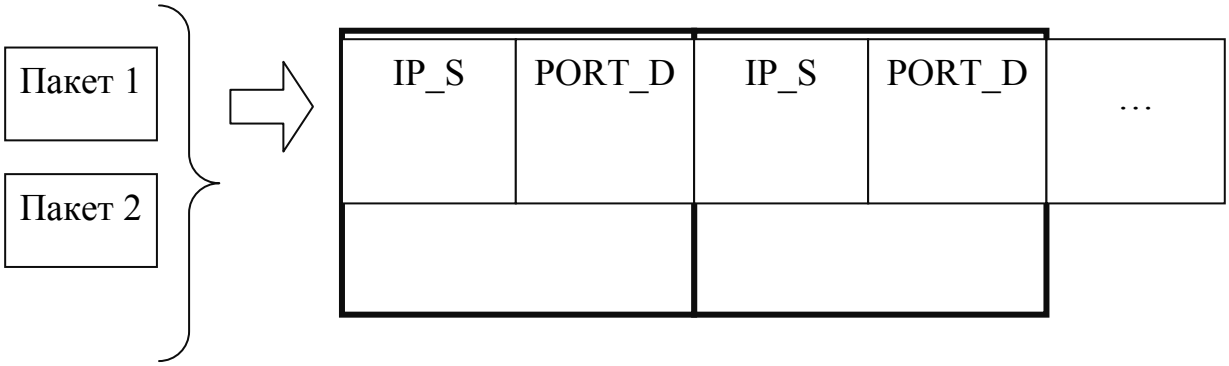

Рис. 1. Структуризація мережевих пакетів

Використання значень ентропії мережевого трафіку для виявлення DDOS-атак базується на порівнянні ентропії трафіку, усередненої за невеликий інтервал часу (локальна міра невизначеності), з відповідною мірою за тривалий проміжок часу (глобальна міра невизначеності), обчисленою без атаки на мережевий сервіс. У випадку, коли локальна міра суттєво відрізняється від відповідної глобальної, імовірність наявності мережевих атак суттєво зростає [3].

Моделювання DDoS-атак виконували на базі спеціально створеної розподіленої мережі з використанням програм netmap, nping та WPEPro. У процесі досліджень мережеві сервіси зазнавали впливу DDOS-атак різного рівня інтенсивності. Збір статистичної інформації проводився за допомогою спеціально розробленої програми-аналізатора на основі відкритих бібліотек WinPcap та jpcap. Приклад базової інформації, що використовувалась для проведення досліджень, представлено у табл. 1.

При цьому, з метою максимального наближення до реальних умов функціонування мережевих сервісів в умовах наявності DDOS-атаки, тестовий трафік складався з суміші реального мережевого трафіку та спеціально змодельованого.

Таблиця 1

Параметри моделювання DDoS-атак

№ послідовності	Розмір послідовності (пакетів)	Час, за який було зібрано пакети, хв.	
		Звичайний режим роботи мережі, хв.	Моделювання атаки, хв.
1	50 000	15	2
2	100 000	30	3
3	150 000	60	5
4	200 000	75	6
5	250 000	84	9

За формулою Шеннона (1) ентропія трафіку залежить від імовірностей 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 типу; N – загальна кількість пакетів трафіку.

При розрахунках за таким класичним алгоритмом виникає необхідність перерахунку частот усіх пакетів при надходженні нового пакета. При великій кількості пакетів це суттєво знижує швидкість обчислень ентропії, що є неприйнятним у випадку наявності DDOS-атаки. Для збільшення швидкості обчислень ентропії мережевого трафіку використовували метод рухомого вікна [4–5]. Схема методу рухомого вікна представлена на рис. 2. Розрахунки ентропії з використанням методу виконуються за наступним алгоритмом (рис. 2). Вибирається вікно розміром W пакетів, обчислюються й зберігаються частоти f_i кожного типу пакетів та визначається базове значення ентропії H_0 для перших W пакетів трафіку. Далі вікно зсувається на величину ΔW вправо вздовж послідовності пакетів, що надходять на мережевий інтерфейс. При цьому фіксуються частоти $f_{before,input}$ і $f_{now,input}$ пакетів, що знаходяться у вікні, і частоти $f_{before,output}$ й $f_{now,output}$ пакетів, що залишились поза межами вікна після його зміщення. За цих умов поточне значення ентропії обчислювали за формулою

$$H_i = H_{i-1} + \Delta H, \qquad (2)$$

де ΔH відображає зміну ентропії при зсуві вікна, (рис. 2)

$$\Delta H = H_i - H_{i-1};$$

$$\Delta H = -\sum_{i=1}^{n} p_i \cdot \log_2 p_i + \sum_{j=1}^{l} p_j \cdot \log_2 p_j ,$$

відповідно

$$\Delta H = -f_{before,input} \cdot \log f_{before,input} -$$
$$- f_{before,output} \cdot \log f_{before,output} +$$
$$+ f_{now,input} \cdot \log f_{now,input} +$$
$$+ f_{now,output} \cdot \log f_{now,output} \cdot$$

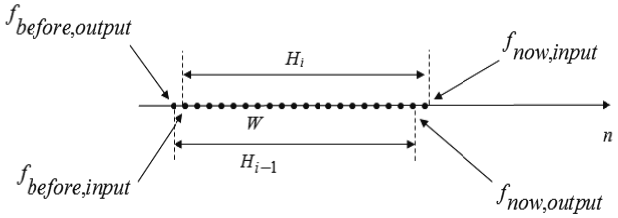

Рис. 2. Схематичне зображення методу рухомого вікна

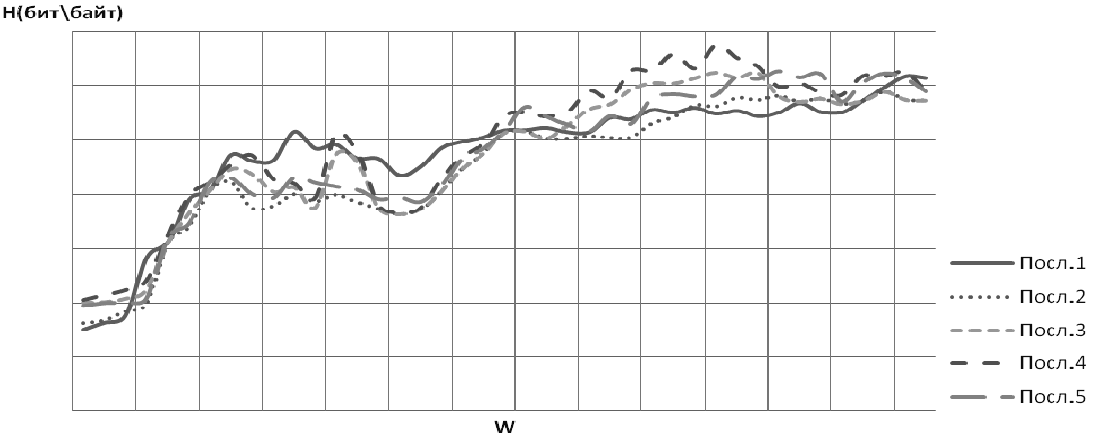

Рис. 3. Залежність ентропії H трафіку від розміру W вікна для різних послідовностей мережевих пакетів

Аналіз отриманих результатів дозволяє зробити висновок про суттєву залежність ентропії від розміру вікна W. Цей параметр у кожному конкретному випадку необхідно визначати експериментально. У даних дослідженнях прийнятний розмір вікна *W=7* визначався шляхом аналізу графіків залежності ентропії досліджуваного трафіку (рис. 3) від розмірів вікна *W*.

Для перевірки можливості використання ентропії трафіку як детектора DDOS-атак, ентропія обчислювалась для мережевого трафіку без атак і при емуляції атаки типу DDOS.

Для цього було задіяно двадцять машин, одна з яких використовувалась як сервер, що обробляв запити клієнтів. Із решти дев'ятнадцяти машин на сервер відправлялися пакети доти, доки не досягалась необхідна кількість пакетів із максимально можливою швидкістю для мережі FastEthernet. Обчислені значення ентропії трафіку без атак та при DDOS-атаці наведено у табл. 2.

Таблиця 2

Ентропія H мережевого трафіка без атаки та при DDoS-атаці

№ послідовності	H без атаки (біт)	H при DDoS-атаці (біт)
1	3,37	1,23
2	3,28	1,5
3	3,23	1,92
4	3,29	1,7
5	3,37	1,85

Висновки. Аналіз отриманих експериментальних результатів дозволяє зробити висновок, що інформаційний аналіз трафіку в реальному масштабі часу може бути використано як ефективний індикатор аномально-

го стану мережі. Зокрема, значення ентропії трафіку є чутливими до DDoS-атак, із розвитком атаки її значення зменшуються майже на 70%. При цьому слід відзначити, що на результати обчислень не впливає розмір пакету. У запропонованій постановці задачі на ентропію впливає сам факт надходження пакету з визначеними параметрами. Відповідно, обчислення ентропії трафіку можна застосовувати в системах виявлення вторгнень IDS, системах управління інформаційною безпекою підприємства, системах підтримки прийняття рішень та ін. Безпосередньо обчисленням повинні передувати декілька підготовчих етапів, зокрема визначення розміру рухомого вікна.

Список літератури / References

1. Skarfone, K. and Mell, P. (20007), *Guide to intrusion detection and prevention systems*, National Institute of Standards and Technology, available at: csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

2. Feinstein, L. and Schnackenberg, D. "Statistical Approaches to DDOS Attack Detection and Response", *Proc. of the DARPA Information Survivability Conference and Expostion (DISCEX'03)*, April 2003.

3. Seong Soo Kim, (2005), "Real-time Analysis of Aggregate Network Traffic for Anomaly Detection", PhD dissertation, Computer Engineering, Yonsei University, available at: http:// cesg.tamu.edu/wp-content/uploads /2012/02/TAMU-ECE-2005-02.pdf

4. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер – СПб.: Питер, 2010. – 943 с.

Olifer, V.G. and Olifer, N.A. (2010), *Kompyuternye seti. Printsypy, tekhnologii, protokoly* [Computer Networks. Principles, Technologies, Protocols], Piter, St.-Petersborg, Russia.

5. Gudkov, O. (2012), "Calculation Algorithm for Network Flow Parameters Entropy in Anomaly Detection. IT Security for the Next Generation", *International Round*, Delft University of Technology, May 11–13, 2012.

Цель. С целью повышения эффективности IDS (intrusion detection systems), ADS (anomaly detection system) и систем управления информационной безопасностью выполнить теоретические и экспериментальные исследования по изучению возможности использования значений вычисленной в режиме реального времени информационной энтропии в качестве базового индикатора атаки на сетевые сервисы.

Методика. Методика работы включает сбор статистической информации о работе IP-сети в нормальном режиме, моделирование процессов, вызывающих аномальные состояния IP-сети, сбор статистической информации о работе сети при наличии DDOS-атак на сетевые сервисы, определение оптимальных размеров подвижного окна, вычисление значений информационной энтропии и их сравнение с эталонными для данной IP-сети.

Результаты. Вычисленные в реальном масштабе времени значения информационной энтропии с использованием метода подвижного окна являются эффективным индикатором аномального состояния IP-сети и могут быть использованы в системах обнаружения вторжений, системах управления информационной безопасностью.

Научная новизна. Предложен алгоритм вычисления информационной энтропии, который, в отличие от классического алгоритма, за счет использования метода подвижного окна позволяет значительно ускорить вычисления и выполнять их в реальном масштабе времени.

Практическая значимость. На основе проведенных теоретических и экспериментальных исследований предложена методика вычислений информационной энтропии, что позволяет использовать этот показатель для анализа сетевого трафика в реальном масштабе времени в IDS, MDS ADS системах.

Ключевые слова: *информационная энтропия, системы обнаружения вторжений, системы обнаружения аномалий, аномальное состояние IP-сети, сетевой трафик, отказы в обслуживании, моделирование, защита информации, безопасность информации*

Purpose. In order to improve the efficiency of IDS (intrusion detection systems), ADS (anomaly detection system) and information security systems management we perform theoretical and experimental studies on the possibility of using the real-time calculated values of information entropy as a basic indicator of attacks of network services.

Methodology. Applied methods include collecting statistical information on IP network normal mode performance, modeling of processes that cause IP network abnormal states, collecting statistical information on the network performance under DDOS-attacks at network services, determining the rolling window optimal size, calculation of information entropy values and their comparison to the reference values for this IP network.

Findings. The values of information entropy calculated in real time with the use of the rolling window method are an effective indicator of anomalous IP network states and can be used for intrusion detection in information security systems management.

Originality. The algorithm for calculating the information entropy allowing significant speeding up the calculations in comparison with the classical algorithm by using a moving window method and performing them in real time has been proposed.

Practical value. The new method of the information entropy computing based on theoretical and experimental studies allows using this indicator to analyze network traffic in real time in IDS, MDS and ADS systems.

Keywords: *information entropy, intrusion detection systems, anomaly detection system, abnormal IP network states, network traffic, denial of service, modeling, information security, information security*

Рекомендовано до публікації докт. техн. наук Л.І. Мещеряковим. Дата надходження рукопису 07.11.12.