DOI 10.31891/2307-5732-2019-271-2-122-127
УДК 004.891

В. М. ДЖУЛІЙ, В. І. ЧОРНЕНЬКИЙ, О. О. САВІЦЬКА
Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ ТА ПРОТИДІЇ РОЗПОДІЛЕНИМ АТАКАМ, СПРЯМОВАНИМ НА ВІДМОВУ В ОБСЛУГОВУВАННІ

В роботі запропоновано актуальний метод та інструментарій для раннього виявлення розподілених атак, спрямованих на відмову в обслуговуванні, і подальшого виявлення шкідливого трафіку на стороні ресурсу, що атакується і його блокування власними силами. Для поділу змішаного трафіку використовується алгоритм кластеризації k-means. Вибір даного алгоритму обґрунтований, проведено доказ його ефективності, підібрані оптимальні характеристики і розмірність даних, вироблені критерії успішності. Розроблені алгоритми складають основу узагальненої методики виявлення DDoS-атак і шкідливого трафіку.

Ключові слова: моделі, алгоритми, ефективність виявлення атак*, метод, мережевий трафік, інформаційна безпека.*

V. M. DZHULIY, V. I. CHORNENKY, O. O. SAVITSKAYA
Khmelnytskyi National University

METHODS OF DETECTION AND COUNTERACTION TO THE DISTRIBUTED ATTACKS AIMED AT FAILURE IN SERVICE

The purpose of the work is to create an actual method and tool for early detection of the distributed attacks aimed at denial of service, and further detection of any harmful traffic directed on the attacked resource and its own blocking. Countermeasures specialized to ensure the security of small and medium-sized resources, have received less development due to the predominance of large severe attacks in the past. And now they are lagging behind the evolution of DDoS attacks themselves. As a part of the method development for detecting DDoSatak and malicious traffic, an original algorithm has been created for detecting a distributed attack at the early stages of a denial of service attack. The algorithm takes into account seasonal deviations in the load, which makes it possible to detect the point of attack in the early stages and with greater accuracy. Besides, research was conducted to confirm the existence of seasonality and to identify any typical seasonal periods. As a result of the research the week, daily and uncertain seasonality and the reasons of its emergence are revealed. It was revealed the tendency of medium and low power attacks on regional resources. The peculiarities of regional level DDoS attacks were investigated and the task of creating a method and software complex for the detection of DDoS attacks and malicious inquiries was solved. The received technique was tested on the data - for legitimate requests, the completeness of the detection was 0.9991 with an accuracy of 0.99811, for malicious inquiries, completeness of 0.9975, accuracy of 0.9924.

Keywords: models, algorithms, attack detection efficiency, method, network traffic, information security.

Вступ

DDoS-атака – розподілена атака, спрямована на відмову в обслуговуванні. В результаті атаки такого типу мережевий ресурс, що атакується, отримує лавиноподібну кількість запитів, які не встигає обробити сервер. Джерелом шкідливих запитів є так звані зомбі-мережі, що складаються переважно з комп'ютерів звичайних користувачів, в силу якихось причин заражених шкідливим програмним забезпеченням. Періодичні повідомлення в засобах масової інформації про недоступність тих чи інших ресурсів в результаті розподілених атак, спрямованих на відмову в обслуговуванні, говорять про неефективність засобів протидії такого роду атак. Також збільшується кількість атак і до невеликих, «середніх» сайтів, які до недавнього часу не становили інтересу для зловмисників. Однак, в даний час, у зв'язку зі збільшенням їх важливості і затребуваності, перебої в їх роботі можуть бути критичними. Разом з цим змінюються і мотиви, які рухають зловмисниками, якщо раніше серед причин виникнення DDoS-атак можна було виділити протест, хуліганство і т.д., то сьогодні все частіше DDoS-атаки є наслідком шантажу і способом вимагання грошей. Це переводить DDoS-атаки з площини одиничних протестних акцій в область кримінального бізнесу, які не обмежується вимаганням, але і є інструментом екстремістських і терористичних організацій [2].

Сьогодні у всьому світі стали звичайною ситуацією атаки на сайти державної влади напередодні виборів або важливих політичних подій [1, 5]. Для паралізації невеликого регіонального ресурсу досить невеликої за потужністю атаки і як наслідок невеликої бот-мережі. Обслуговування та підтримка таких бот-мереж є менш витратним, і потенційно створити такі мережі може більшість зловмисників. Цей факт на фоні відсутності адекватних засобів протидії робить загрози безпеки регіональних ресурсів в результаті DDoS-атак особливо значущими. З одного боку, для протидії таким атакам можуть бути ефективно застосовані засоби, призначені для відображення великих атак. З іншого – впровадження і підтримка таких засобів є економічно затратною і не по кишені регіональним ресурсам. Засоби протидії, спеціалізовані саме на забезпечення безпеки невеликих і середніх ресурсів, отримали менший розвиток через переважання в минулому саме великих атак. І в даний час відстають від еволюції самих DDoS-атак [6].

Відповідно до звіту, опублікованого компанією «Лабораторія Касперського», число DDoS-атак постійно збільшується [3, 4]. Так, наприклад, за друге півріччя 2017 р. значно збільшилася кількість атак. При цьому збільшилася і потужність проведених атак, в порівнянні з першим півріччям вона виросла на 57%.

Разом з кількістю і потужністю постійно зростає і складність самих атак. Зловмисники шукають принципово нові методи проведення атак, і дуже часто існуючі засоби захисту виявляються безсилими перед ними. Так, наприклад, порівняно новий вид DDoS-атак – THC-SSL-DOS – експлуатує особливості SSL протоколу і дає можливість одному комп'ютеру зробити недоступним сервер середньої конфігурації [3]. В

2017 р. був атакований сайт американської біржі Nasdaq. В результаті атаки сайт повністю перестав реагувати на запити. При цьому біржа Nasdaq є найбільшою електронної фондовою біржею США і другою в світі за величиною ринкової капіталізації [5]. Україна також не відстає від світової тенденції зростання DDoS-атак, а по деяких позиціях займає навіть перші місця. За повідомленнями засобів масової інформації, з лютого по березень 2017 р. з України було проведено понад 2,4 мільйона кібер-атак.

Найбільш характерним проявом DDoS-атак є «затоплення» або flooding каналу зв'язку або конкретного мережного пристрою величезною кількістю мережевих пакетів. В залежності від типу пакетів, це може призвести до перевантаження каналу і, як наслідок, неможливості проходження по ньому легітимного трафіку, або до підвищеної завантаженості пристрою (заповнення доступного обсягу оперативної пам'яті і завантаження ресурсів процесора).

При достатніх обчислювальних і серверних потужностях, можливо зробити перенаправлення трафіку назад до атакуючого. Цей метод досить складний в реалізації і вимагає не тільки хорошої матеріальної бази, а й високої кваліфікації адміністратора серверного ресурсу.

Постановка задачі

В результаті проведеного дослідження відмічено, що в даний час значно збільшилася кількість DDoS-атак середньої і малої інтенсивності, спрямованих, як правило, на регіональні ресурси. Це збільшення цілком прогнозовано - з розвитком мережі збільшується потенційна кількість можливих жертв. Крім того, вдосконалюється сам механізм проведення атак. Для зловмисника проведення атаки вже не є настільки складним. А зомбі-комп'ютери намагаються емулювати дії самих користувачів. Все це веде до загального збільшення числа атак.

Аналіз засобів протидії показав, що в даний час більший розвиток отримала група засобів протидії, призначена для відбиття потужних атак. У цю групу входять, як правило, дорогі засоби, призначені для великих провайдерів або компаній. Засоби протидії невеликим і середнім атакам, що розміщенні на сервері, представлені в незначній кількості. При цьому аналіз вхідного трафіку на рівні додатків може бути більш ефективним. З одного боку, проведення такого аналізу економічно менш затратно, з іншого – може бути цілком достатнім для відбиття малих і середніх атак, тенденція домінування яких вже намітилася.

Основна частина

Оптимальним рішенням для виявлення початку атаки і подальшого виявлення шкідливого трафіку буде рішення, засноване на аналізі аномалій, в результаті якого відбувається порівняння поточного стану системи з її нормальним станом. Порівняння станів системи в контексті DDoS-атак можна проводити шляхом порівняння різних властивостей мережевої активності. До цих властивостей можуть бути віднесені: кількість запитів, тип запитів, кількість запитів певного типу або протоколу, IP адреса джерела, швидкість надходження запитів, їх час і т.д.

Нехай множина $A\left(a_1, a_2, a_3, ..., a_n\right)$ – набір всіх можливих властивостей для всіх мережевих клієнтів. Множина $B\left(b_1, b_2, b_3, ..., b_m\right)$ – множина легітимних клієнтів конкретного мережевого ресурсу. Кожен мережевий клієнт має набір індивідуальних властивостей. Наприклад, клієнт b_1 має властивості $A1\left(a_4, a_8, a_{10}, a_{14}\right)$, клієнт b_2 має властивості $A2\left(a_3, a_8, a_{11}, a_{14}\right)$ і т.д. Дані властивості представляють набір підмножин множини A. Перетин всіх цих підмножин характеризує клієнтів мережевого ресурсу, за якими вони можуть бути класифіковані. Точно так нелегітимні клієнти матимуть свій набір властивостей, за яким вони також можуть бути класифіковані.

На сьогоднішній день DDoS-атаки ускладнюються, і зловмисники намагаються повністю імітувати поведінку легітимних клієнтів. У цій ситуації перевагу при аналізі властивостей мережевої активності необхідно віддати тим властивостям, які не можуть бути підроблені зловмисниками. При нестачі таких властивостей необхідно вводити штучні властивості, наприклад, проходження модифікації тест Тьюринга – введення даних з картинки.

Таким чином, завдання по визначенню і виявлення шкідливих запитів в контексті даної роботи зводиться до їх класифікації на підставі властивостей мережевої активності. Оптимальним рішенням для виявлення шкідливого трафіку є використання різних класифікаторів і нейронних мереж. Складністю в реалізації даного рішення є той факт, що для нормального функціонування класифікатора потрібно мати дві актуальні навчальні вибірки, відповідно шкідливому і легітимному трафіку. Однак до моменту початку атаки отримати ці вибірки не представляється можливим. Це цілком очевидно для вибірки, що відповідає шкідливому трафіку, так як до початку атаки шкідливі запити відсутні. Але це також справедливо і для вибірки, що характеризує легітимний трафік. Так як мережева картина постійно змінюється, буде змінюватися і вміст вибірки відповідного легітимного трафіка. Таким чином, вибірка по легітимності трафіка, наприклад, місячної давності, може бути не актуальна для поточної мережевої ситуації. Крім того, є ризик, що в цій вибірці можуть виявитися дані, відповідні шкідливим запитам, що в подальшому викличе помилки в роботі класифікатора.

Дана проблема актуальна, тому що зловмисник може спеціально почати підмішувати до легітимного трафіку незначне число шкідливих запитів, які не зможуть бути ідентифіковані як початок атаки, але зможуть негативно «навчити» вибірку, що характеризує легітимний трафік. Для подолання цієї проблеми необхідно точно визначити точку початку атаки. Це дасть можливість весь попередній трафік віднести до легітимного і відкриє додаткові можливості по розділенню змішаного трафіку, який приходить після початку атаки, на легітимний і шкідливий.

В цьому випадку методика виявлення шкідливого трафіку, в першому наближенні, буде зводитися до наступних кроків: визначаємо актуальні сезонні періоди; з урахуванням сезонності визначаємо точку початку атаки; відносимо весь попередній перед початком атаки трафік до легітимного; класифікуємо змішаний трафік на легітимний і шкідливий; порівнюємо легітимний трафік виділений зі змішаного з трафіком що надійшов до початку атаки; на підставі результатів, отриманих на попередньому кроці і вироблених критеріїв успішності, коригуємо вибірки; весь вступний трафік аналізуємо з урахуванням отриманих даних.

Початок DDoS-атаки пов'язаний зі збільшенням числа запитів до атакованого сервера. Таким чином, для фіксації факту атаки необхідно встановити границю по кількості запитів до сервера, при порушенні якої однозначно буде фіксуватися нештатна ситуація. Такою границею може виступати максимальна кількість запитів до сервера, плюс деякий запас можливих запитів. Можливість установки граничної межі, після якої буде відбуватися оповіщення адміністраторів, активація необхідних модулів і т.д., реалізована в різних мережевих засобах як програмного, так і апаратного рівня. При цьому такий підхід має ряд мінусів:

1. Для запобігання випадкових спрацьовувань, межа що встановлюється повинна бути істотно вище максимального рівня кількості запитів. Що, в свою чергу, призводити до виникнення похибки при виявленні атаки.

2. Мережевий ресурс може відчувати різне навантаження в залежності від часу доби і днів тижня. В цьому випадку атака, що почалася в період затишшя, наприклад, у вихідний день або вночі, буде зафіксована із запізненням. Якщо в системі запобігання вторгнень передбачено використання класифікаторів та навчання фільтрів на підставі вхідного трафіку, є ймовірність в їх негативному навчанні.

Для вирішення зазначених проблем необхідно використовувати ковзаючу оцінку, що характеризує поточну мережеву активність. На підставі цієї оцінки встановлювати динамічну границю, актуальну для періоду можливого початку атаки. В якості ковзаючої оцінки можливо використовувати середньоквадратичне відхилення:

$$\sigma = \sqrt{\frac{1}{n} \cdot \sum_{i=1}^{n} \left(x_i - \bar{x} \right)^2} \ , \tag{1}$$

де σ – середньоквадратичне відхилення; n – кількість розглянутих часових періодів; x_i – кількість запитів за i-період;

$\bar{x}$ – середнє арифметичне запитів по всіх періодах.

В результаті експериментів, було встановлено, що для різних сайтів оптимальне значення верхньої межі може відрізнятися і перебувати, як правило, в діапазоні від 2.2σ до 2.9σ. З цієї причини, для більш гнучкого налаштування програмного забезпечення по виявленню початку DDoS-атаки, цей параметр задається не жорстко. У оператора програмного комплексу є можливість варіювати значення даного параметра. Однак такий підхід також має потенційну вразливість, пов'язану з тим, що зловмисник може поступово нарощувати потужність атаки, зрушуючи при цьому границю середньоквадратичного відхилення. усунути дану вразливість може облік сезонних коливань.

Такий підхід дозволяє сформувати досить точну верхню межу, порушення якої може бути витлумачено як виникнення мережевої аномалії. Збільшення точності дозволяє зменшити час, необхідний для виявлення атаки, і досить точно зафіксувати її початок.

Крім того, в рамках такого підходу виключаються можливості негативного навчання фільтрів і спрацьовування системи виявлення з запізненням шляхом поступового нарощування потужності атаки. Так як межа в цьому випадку буде будуватися за схожими сезонним періодами. Наприклад, поступове нарощування потужності атаки протягом дня буде зафіксовано при порівнянні кількості запитів з кількістю запитів актуальних сезонних періодів за минулу добу.

Виявлення і дослідження сезонності. В рамках раннього виявлення початку атаки, і з огляду на перспективність підходу необхідно враховувати сезонні коливання, провести додаткове дослідження, що вивчає сезонні коливання кількості запитів до мережевих Internet ресурсів. Основним завданням дослідження був доказ існування сезонних періодів в роботі web-сайтів. А також вирішення питання, чи може випадковий сплеск в відвідуваності Internet ресурсу, викликаний, наприклад, публікацією на нього посилання з високо відвідуваного ресурсу, викликати порушення сезонності, і, як наслідок, помилкове спрацьовування.

В результаті дослідження для поділу змішаного трафіку на легітимний і шкідливий обраний метод кластеризації на основі алгоритму k-means. Метод забезпечує прийнятну точність, мінімальне навантаження і оптимальну швидкість роботи. Даний алгоритм дозволяє провести кластеризацію при заздалегідь відомому числі кластерів. Алгоритм має прийнятну точність, необхідну для первинного поділу, і більш високу швидкість роботи, порівнянню з іншими алгоритмами.

Суть алгоритму полягає в виділення двох кластерів і обчисленні їх центрів мас, на наступних ітераціях відбувається корекція кластерів (перенесення елементів в відповідно до розрахованих центрів мас) і перерахування центрів мас.

$$V = \sum_{i=1}^{k} \sum_{x_j \in S_i} \left(x_j - \mu_i \right)^2 \ , \tag{2}$$

де k – число кластерів;

S_i – отримані кластери, i – 1,2, … , k_i ;

μ_i – центри мас векторів $x_j \in S_i$.

В результаті роботи алгоритму змішаний трафік буде розділений на два кластера, відповідних легітимному і шкідливому трафіку.

Таким чином, на даному етапі доступні для аналізу і обробки три групи трафіку:

1. Відповідно, легітимному трафіку, що передує початку атаки – *T*.
2. Відповідно, легітимному трафіку, виділений із змішаного трафіку – *T**.
3. Відповідно шкідливому трафіку, виділений із змішаного трафіку – *H*.

Критерії успішності, корекція отриманих кластерів. Для оцінки ефективності кластеризації розглянемо рівняння стаціонарних ймовірностей:

$$\begin{aligned}
&p_0\lambda = p_1\mu \\
&(\lambda + i\mu)\, p_i = \lambda p_{i-1} + (i+1)\cdot \mu p_{i+1},\ i = 1,...,K-2, \\
&\left(\lambda + (K-1)\mu\right) p_{K-1} = \lambda p_{K-2} + K\widetilde{N}\cdot \mu p_K, \\
&\left(\lambda^* + K\widetilde{N}\mu\right) p_K = \lambda p_{K-1} + K\widetilde{N}\cdot \mu p_{K+1}, \\
&\left(\lambda^* + i\mu^*\right) p_i = \lambda^* p_{i-1} + (i+1)\cdot \mu^* p_{i+1},\ i = K+1,...,N-1
\end{aligned} \tag{3}$$

де λ – інтенсивність навантаження;

λ_L – інтенсивність навантаження, створювана легальними користувачами;

S – інтенсивність шкідливого трафіку, μ – інтенсивність звільнення черги запитів;

μ^* – інтенсивність звільнення черги запитів при активованому фільтрі,

K – межа активації фільтра;

N – обсяг черги запитів;

$\lambda = \lambda_L + S$ – навантаження в момент атаки;

$\lambda^* = \lambda_L + S(1 - E_2)$ – навантаження при активованому фільтрі;

E_1, E_2 – помилки першого і другого роду,

При нормуванні $\sum_{i=1}^{N} p_i = 1,$ отримаємо ймовірність блокування запиту.

$$p_{BLK} = \frac{\frac{1}{N!}\left(\frac{\lambda}{\mu}\right)^{K-1} \frac{\lambda}{\mu^*}\left(\frac{\lambda^*}{\mu^*}\right)^{N-K}}{\sum_{i=0}^{K-1} \frac{\left(\frac{\lambda}{\mu}\right)^{i}}{i!} + \sum_{i=K}^{N} \frac{1}{i!}\left(\frac{\lambda}{\mu}\right)^{K-1} \frac{\lambda}{\mu^*}\left(\frac{\lambda^*}{\mu^*}\right)^{i-K}} \tag{4}$$

Таким чином, ефективність поділу шкідливого і легітимного трафіку можна оцінити як $R = (1 - E_1)\cdot(1 - p_B)$.

На підставі отриманої оцінки, були вироблені критерії успішності.

На наступному кроці алгоритму проводиться корекція отриманих вибірок з урахуванням наступних критеріїв:

1. Критерій розмірності отриманих кластерів. Якщо в поточному періоді, що відноситься до атаки, кількість запитів – *n*, а в аналогічних сезонних періодах, що відносяться до легітимного трафіку – *m*, то кількість шкідливих запитів буде наближено рівним *n-m*. Це ж справедливо і для різних властивостей мережевої активності (кількість запитів до цільової сторінки, цільового порту, за певним протоколом і т.д.)

2. Критерій схожості легітимних вибірок. Максимальна схожість легітимної вибірки, що передує початку атаки, з легітимною вибіркою, виділеної зі змішаного трафіку.

3. Критерій відповідності центрів мас. Центр мас надійної вибірки, виділеної із змішаного трафіку, повинен відповідати аналогічному сезонному періоду надійного трафіку, що передує початку атаки. Іншими словами, відстань між цими центрами мас повинена наближатися до нуля. Для подальшого уточнення можна розрахувати ймовірність приналежності кожного елемента своєму класу. Елементи з найменшою ймовірністю переносяться в протилежні групи з урахуванням критерію розмірності груп.

Для розрахунку схожості надійних кластерів і надалі для класифікації запитів, що надходять можна скористатися «Байєсовким класифікатором». В якості ймовірнісної моделі для класифікатора використовуємо умовну ймовірність $p(C \mid F_1,...,F_n)$ над залежною змінною класу *C* з малою кількістю результатів або *класів*, що залежить від декількох змінних $F_1,...,F_n$. Використовуючи теорему Байєса, запишемо:

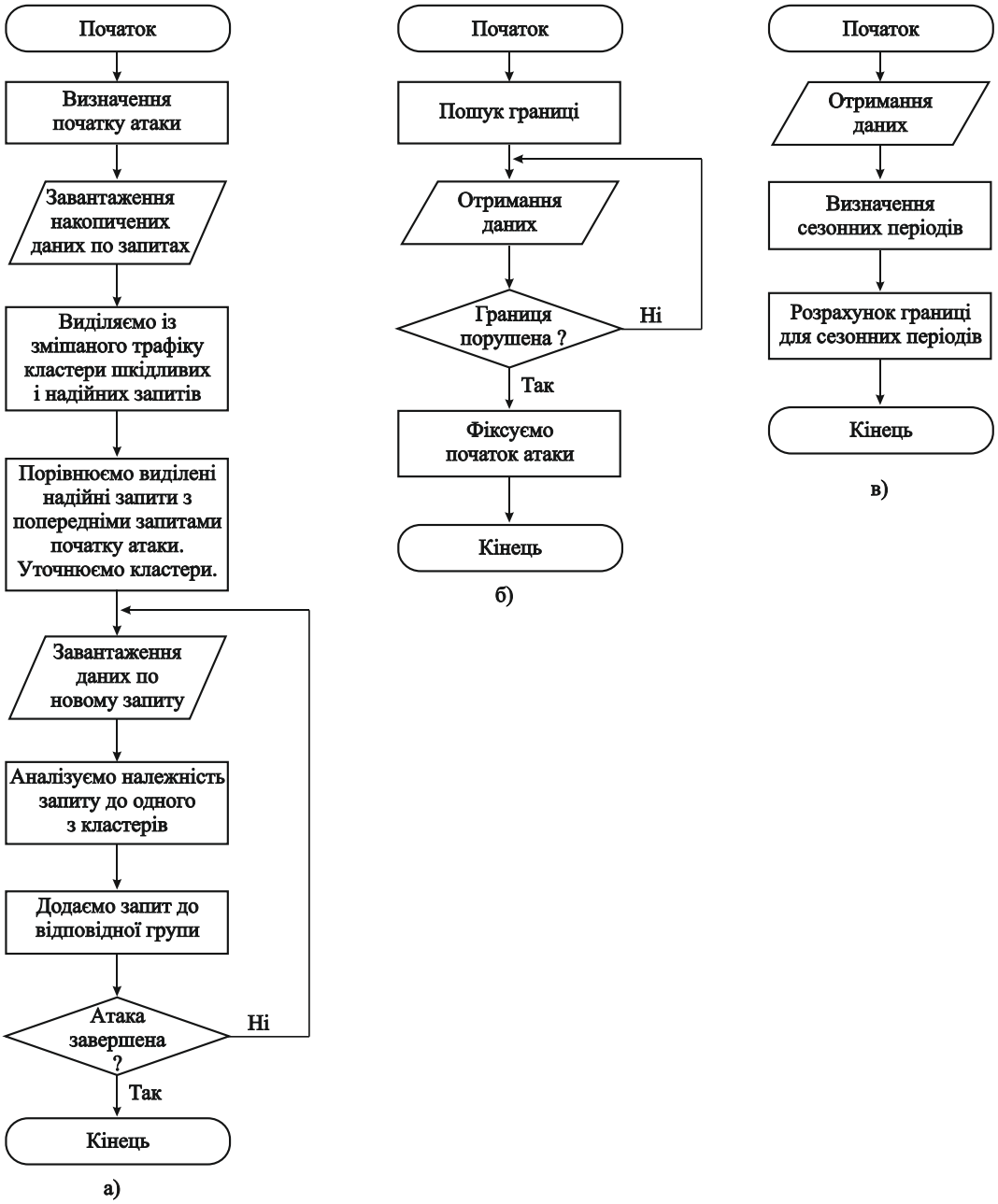

Рис. 1. Алгоритми р визначення початку атаки і виділення шкідливого трафіку

$$p(C \mid F_1,...,F_n) = \frac{p(C) \cdot p(F_1,...,F_n \mid C)}{p(F_1,...,F_n)}$$

Умовний розподіл по класовій змінній C може бути виражено так:

$$p(C \mid F_1,...,F_n) = \frac{1}{Z} p(C) \prod_{i=1}^{n} p(F_i \mid C)$$

Таким чином, для класифікації трафіку за двома класами отримаємо:

$P(T \mid D) = \frac{P(T)}{P(D)} \prod_{i=1}^{n} P(w_i \mid T)$ – для класу надійних користувачів;

$P(H \mid D) = \frac{P(H)}{P(D)} \prod_{i=1}^{n} P(w_i \mid H)$ – для класу ненадійних користувачів.

В якості навчальних вибірок використовуються множина T і множина H. Після закінчення цього кроку елементи з множини T*, віднесені до групи шкідливого трафіку, міняються місцями з елементами множини H з урахуванням зазначених вище критеріїв. Даний крок повторюється до тих пір, поки всі елементи множини T не будуть позначені як легітимні, або поки алгоритм не досягне порогового значення ітерацій.

Отримані вибірки, відповідні легітимному і шкідливому трафіку, а також механізм їх підтримки в актуальному стані дозволяють використовувати їх з різними класифікаторами. На рис. 1 показані

принципові схеми алгоритмів по визначенню початку атаки і виділенню шкідливого трафіку. Перша схема (рис. 1 а) пояснює алгоритм виділення шкідливого трафіку, друга (рис. 1 б) і третя (рис. 1 в) – алгоритми визначення початку атаки.

На першому кроці відбувається виклик підпрограм по виявленню сезонних періодів, розрахунку для них допустимої межі кількості запитів, і визначення початку атаки. У разі початку атаки, алгоритм повинен розподілити змішаний трафік на два кластери, один містить шкідливі запити, інший надійні запити. Дані кластери уточнюються. Нові запити аналізуються на приналежність того або іншому кластеру і за результатом додаються до відповідного кластеру.

Висновки

В рамках розробки методу виявлення DDoSатак і шкідливого трафіку розроблений оригінальний алгоритм виявлення на ранніх стадіях точки початку розподіленої атаки, спрямованої на відмову в обслуговуванні. Алгоритм враховує сезонні відхилення в навантаженні, що дає можливість виявляти точку початку атаки на ранніх стадіях і з більшою точністю. Додатково проведено дослідження, спрямоване на підтвердження існування сезонності і виявлення типових сезонних періодів. В результаті дослідження виявлені тижнева, добова і невизначена сезонність і причини її виникнення.

Розроблено метод отримання навчальних вибірок та класифікації трафіку, що надходить, на групи шкідливих і легітимних запитів. Для поділу змішаного трафіку використовується алгоритм кластеризації k-means. Вибір даного алгоритму обгрунтований, проведено доказ його ефективності. Для алгоритму підібрані оптимальні характеристики і розмірність даних, вироблені критерії успішності. Розроблені алгоритми складають основу узагальненої методики виявлення DDoS-атак і шкідливого трафіку, яка в загальному вигляді може бути описана так: за допомогою статистичних даних, визначаємо існуючі сезонні періоди; для кожного сезонного періоду визначаємо допустиму верхню межу кількості запитів; у разі порушення границі, фіксуємо точку початку атаки; відносимо весь, що передує початку атаки, трафік до кластеру, відповідного легітимного трафіку; за допомогою алгоритму k-means класифікуємо змішаний трафік на легітимний і шкідливий; порівнюємо трафік, що передує початку атаки, з кластером, легітимного трафіку, виділеного зі змішаного трафіку; на підставі результатів, отриманих на попередньому кроці, і з урахуванням вироблених критеріїв успішності, коригуємо кластери; весь трафік, що надходить, аналізуємо з урахуванням отриманих в попередньому пункті результатів.

Література

1. Бабаш А.В. Криптографические методы защиты информации : учебник для студ. вузов / А. В. Бабаш, Е. К. Баранова. – М. : КНОРУС, 2016. – 190 с.

2. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М. : Юридическая литература, 2006. – 160 с.

3. Борисов М.А. Основы программно-аппаратной защиты информации : учеб. пособие для вузов / М.А. Борисов, И.В. Заводцев, И.В. Чижов. – 4-е изд., перераб. и доп. – М. : ЛЕНАНД, 2016. – 416 с.

4. Васильева И.Н. Криптографические методы защиты информации : учебник и практикум для академ. бакалавриата / И.Н. Васильева. – Санкт-Петерб. гос. эконом. ун-т . – М. : Юрайт, 2017. – 349 с.

5. Нестеров С.А. Основы информационной безопасности : учебник / С. А. Нестеров. – СПб : Лань, 2017. – 423 с.

6. Олифер В.Г. Безопасность компьютерных сетей / В.Г. Олифер, Н.А. Олифер. – М. : Горячая линия-Телеком, 2017. – 644 с.

7. Тихоненко О.М. Модели массового обслуживания в информационных системах : учебное пособие для ВУЗов / О.М. Тихоненко. – Минск : Технопринт, 2003. – 327 с.

8. Шаньгин В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М. : ДМК Пресс, 2017. – 702 с.

References

1. Babash A.V. Kriptograficheskie metody zashhity informacii : uchebnik dlja stud. vuzov / A. V. Babash, E. K. Baranova. – M. : KNORUS, 2016. – 190 s.

2. Baturin Ju.M. Komp'juternaja prestupnost' i komp'juternaja bezopasnost' / Ju.M. Baturin, A.M. Zhodzinskij. – M. : Juridicheskaja literatura, 2006. – 160 s.

3. Borisov M.A. Osnovy programmno-apparatnoj zashhity informacii : ucheb. posobie dlja vuzov / M.A. Borisov, I.V. Zavodcev, I.V. Chizhov. – 4-e izd., pererab. i dop. – M. : LENAND, 2016. – 416 s.

4. Vasil'eva I.N. Kriptograficheskie metody zashhity informacii : uchebnik i praktikum dlja akadem. bakalavriata / I.N. Vasil'eva. – Sankt-Peterb. gos. jekonom. un-t . – M. : Jurajt, 2017. – 349 s.

5. Nesterov S.A. Osnovy informacionnoj bezopasnosti : uchebnik / S. A. Nesterov. – SPb : Lan', 2017. – 423 s.

6. Olifer V.G. Bezopasnost' komp'juternyh setej / V.G. Olifer, N.A. Olifer. – M. : Gorjachaja linija-Telekom, 2017. – 644 s.

7. Tihonenko O.M. Modeli massovogo obsluzhivanija v informacionnyh sistemah : uchebnoe posobie dlja VUZov / O.M. Tihonenko. – Minsk : Tehnoprint, 2003. – 327 s.

8. Shan'gin V.F. Informacionnaja bezopasnost' i zashhita informacii / V.F. Shan'gin. – M. : DMK Press, 2017. – 702 s.

Рецензія/Peer review : 15.3.2019 р. Надрукована/Printed :10.4.2019 р.
Рецензент: д. т. н., проф. Мясіщев О. А.