DOI 10.31891/2307-5732-2019-273-3-180-187
УДК 621.391 160164

С.М. ЛИСЕНКО, В.А. ТКАЧУК
Хмельницький національний університет

МЕТОД ТА ПРОГРАМНІ ЗАСОБИ ВИЯВЛЕННЯ КІБЕРАТАКИ ТИПУ R.U.D.Y. НА ОСНОВІ ВИКОРИСТАННЯ АЛГОРИТМУ ВИЗНАЧЕННЯ САМОПОДІБНОСТІ ТРАФІКУ

В роботі представлено метод виявлення DoS-атаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності мережевого трафіку. Використання запропонованого методу дозволяє здійснювати виявлення DoS-атаки на прикладному рівні моделі OSI. Запропонований метод може бути основою для побудови програмного забезпечення систем виявлення кібератак.

Ключові слова: DoS-атака, R.U.D.Y., R-U-Dead-Yet, виявлення кібератак, показник Херста, самоподібність трафіку.

S. LYSENKO, V. TKACHUK
Khmelnytskyi National University

METHOD AND SOFTWARE FOR DETECTING R.U.D.Y. ATTACK BASED ON THE USAGE OF THE ALGORITHM OF DETERMINING TRAFFIC SELF-SIMILARITY

Antivirus software using signature-based technologies can not normally detect harmful zero-day software, since such new signatures are not available for newly created malware. An analysis of known methods to combat cyberattacks shows their lack of efficiency, so building a new method for detecting cyber-threats is an extremely urgent task. The article presents a new method for detecting a DoS-attack type R.U.D.Y. using the algorithm to determine the self-similarity of network traffic. In the enlarged version of the presentation of the algorithm, the method consists of two parts: the study of the neural network of previously received data about harmful traffic and the analysis of the received network traffic to form conclusions about the possible detection of cyber attacks. Moreover, in order to improve the efficiency of the method, it is expedient to implement the first part before the actual monitoring of network traffic, as the training of the neural network requires a certain amount of time during which the received harmful traffic can be analysed with insufficient efficiency. As the approach uses the neural networks there are several factors, which can predict prediction accuracy. One of them is the diversity of training samples Most conspicuously, that not all possible feature vectors, that describe different cyberattacks, are adequately represented in the training set. Thus, system can be further improved by choosing more than a few malicious samples for each attack classes. The described method makes it possible to detect harmful streams of data packets among ordinary, and continuous monitoring of certain malicious flows makes it possible to detect an attacker and allows to isolate the usual network data stream from the harmful one. In the enlarged version of the presentation of the algorithm, the method consists of two parts: the study of the neural network of previously received data about harmful traffic and the analysis of the received network traffic to form conclusions about the possible detection of cyber attacks.

Keywords: DoS-attack, R.U.D.Y., R-U-Dead-Yet, cyberattacks detection, Hurst exponent, traffic self-similarity.

Вступ

Ефективне налаштування мережевих каналів зв'язку для запобігання та виявлення DoS-атак або інших аномалій мережевого трафіку є надзвичайно важливою задачею для здійснення ефективного управління комп'ютерною мережею. Для ефективної роботи значної частини існуючих механізмів виявлення DoS-атак потрібна наявність великого об'єму мережевого трафіку. В такому випадку, при використанні таких механізмів захисту, повільні DoS-атаки, які генерують відносно малий об'єм трафіку, залишаються невиявленими.

Прикладами можливих методів виявлення повільних DoS-атак є методи виявлення за допомогою визначення закономірностей в мережевому трафіку. Одним з таких методів є метод виявлення DoS-атак за допомогою визначення ступеня самоподібності трафіку. Такий метод дозволяє визначати прихований шкідливий трафік поміж звичайного у режимі реального часу.

Алгоритм визначення самоподібного трафіку дає можливість виявити шкідливі потоки пакетів серед звичайних, а постійний моніторинг визначених шкідливих потоків може привести до виявлення зловмисника та дозволить ізолювати звичайний TCP-потік від шкідливого.

Використання подібних методів виявлення DoS-атак на мережевому рівні моделі OSI дає можливість використовувати переваги масштабованості, що забезпечує захист тих вузлів мережі, в яких немає власних внутрішніх механізмів захисту.

Пов'язані роботи

Відмінною особливістю деяких DoS-атак прикладного рівня моделі OSI, таких як R.U.D.Y., є генерація невеликого об'єму мережевого трафіку, що ускладнює використання традиційних інструментів виявлення DoS-атак. Повільний мережевий трафік також дозволяє більш ефективно приховувати проведення такої DoS-атаки від тих механізмів захисту, принцип дії яких заснований на аналізі високошвидкісного трафіку. Саму тому було проведено ряд досліджень з метою визначення нових механізмів виявлення повільних DoS-атак.

Так, наприклад, у роботі [1] були представлені можливі механізми виявлення повільних DoS-атак, серед яких метод виявлення на основі визначення самоподібності трафіку. Як зазначено у даній роботі, ефективність виявлення DoS-атак методом визначення самоподібності значною мірою залежить від бази даних сигнатур, використовуваних для порівняння трафіку та самих алгоритмів порівняння. Також було

зазначено, що перевагою такого методу є можливість масштабування, а недоліком є потреба в додаткових ресурсах оперативної пам'яті.

Властивість самоподібності трафіку, яка лежить в основі розроблюваного методу виявлення кібератаки типу R.U.D.Y. була досліджена у роботах [2] та [3]. В даних роботах було доведено, що для мережевого трафіку характерна властивість самоподібності, яка відображається у вигляді структурної подібності на протязі усіх часових відрізків, протягом яких був здійснений моніторинг Ethernet трафіку.

Реалізація та опис можливого алгоритму виявлення DDoS-атак на основі визначення самоподібності трафіку були представлені у роботі [4]. Результати проведених експериментів показують, що методи виявлення на основі самоподібності дають можливість виявляти шкідливий трафік поміж звичайного у режимі реального часу.

У роботі [5] був проведений статистичний аналіз Ethernet LAN трафіку та було надане пояснення виникнення самоподібності з точки зору фізики. Аналогічні дослідження були проведені та описані у роботі [6] для високошвидкісного трафіку.

У роботі [7] представлений приклад використання методів машинного навчання для виявлення кібератаки типу R.U.D.Y. за допомогою визначення характеристик мережевої поведінки даної атаки на мережевому рівні моделі OSI. Як зазначено у даній статті, найбільш важливими характеристиками поведінки, за якими можливе виявлення атаки є розмір трафіку, самоподібність між пакетами та швидкість передачі даних. При чому у роботі було зазначено, що значна частина механізмів захисту від таких DoS-атак включають в себе також моніторинг розподілення та використання системних ресурсів сервера, таких як завантаженість центрального процесора та оперативної пам'яті, а також моніторинг відкритих мережевих з'єднань.

Самоподібність мережевого трафіку

В загальному випадку мережевий трафік можна представити у вигляді фракталу. В широкому розумінні фрактал означає фігуру, малі частини якої в довільному збільшенні є подібними до неї самої. Іншими словами певний об'єкт або явище можна вважати самоподібним, якщо має місце точний або наближений збіг такого об'єкта або явища з частиною самого себе. Важливою властивістю будь-якого фракталу, а отже і мережевого трафіку є властивість самоподібності. Так як мережевий трафік можна масштабувати тільки до певної фізичної межі, то властивість самоподібності трафіку також зберігається до певної межі.

Самоподібність мережевого трафіку проявляється у вигляді схожості частоти отриманих пакетів даних в різних часових масштабах, що при різному масштабуванні нагадує форму фракталу.

Через те що самоподібність є випадковим процесом, ступінь самоподібності може бути визначений за допомогою так званого коефіцієнта Херста.

Коефіцієнт Херста

Для визначення ступеня самоподібності трафіку був використаний так званий коефіцієнт Херста. В загальному випадку даний коефіцієнт представляє собою величину, яка характеризує схильність певного процесу до слідування певним тенденціям. Стосовно визначення самоподібності трафіку, коефіцієнт Херста представляє собою величину, яка використовується для аналізу часових рядів, протягом яких був здійснений збір мережевого трафіку.

Коефіцієнт Херста може приймати значення від 0 до 1. Зменшення цієї величини означає що затримка між двома однаковими парами значень в часовому ряді збільшується. Послідовності, для яких H > 0,5, зберігають наявну тенденцію, тобто зростання в минулому більш імовірно призведе до зростання в майбутньому, і навпаки. При значенні 0,5 явної тенденції не виражено, а при менших значеннях будь-яка тенденція прагне змінитися на протилежну.

Дана величина визначається як функція відрізку часу часового ряду наступним чином:

$$\mathrm{E}\left[\frac{\mathrm{R}(n)}{\mathrm{S}(n)}\right] = \mathrm{C}n^{H},\ n \to \infty,$$

де $\mathrm{R}(n)$ – розмах накопичених відхилень перших *n* значень від середнього значення ряду;

$\mathrm{S}(n)$ – стандартне відхилення;

$\mathrm{E}[x]$ – математичне очікування;

n – величина проміжку часу;

C – константа.

Для найбільш точного визначення коефіцієнта Херста, часовий відрізок повинен бути достатньо великим. Тому ефективність виявлення DoS-атаки методом визначення самоподібності трафіку значно залежить від величини проміжку часу, протягом якого був здійснений збір та аналіз мережевого трафіку.

Математичне пояснення самоподібності мережевого трафіку

Якщо надходження мережевого трафіку представити у вигляді випадкового процесу, то такий процес можна розділити на дискретні проміжки часу у вигляді $\mathrm{X} = (X_1,\ X_2, \ldots)$. Якщо проміжки часу прийняти рівними *n*, то такий випадковий процес буде мати вигляд $\mathrm{X}^{(n)} = (X_1^n, X_2^n, \ldots)$, компоненти якого

визначаються за формулою:

$$X_k^{(n)} \triangleq \frac{\left(X_{kn-n+1}+\ldots+X_{kn}\right)}{n}, n,k \in N$$

Для опису залежності випадкових процесів X та $X^{(n)}$ доцільно визначити коефіцієнти кореляції $r(q)$, який описує залежність процесу X та коефіцієнт $r_n(q)$, який описує процес $X^{(n)}$. В загальному випадку процес X можна вважати самоподібним, якщо коефіцієнт Херста приймає значення від 0,5 до 1 та виконується рівність:

$$r_n(q) = r(q), n \in Z, n \in \{2,3,\ldots\}$$

В такому випадку, самоподібний процес X є дуже схожим до процесу $X^{(n)}$, так як коефіцієнт кореляції $r(q)$ не змінюється після виконання масштабування по часовим відрізкам довжиною *n*. Іншими словами, частота отримання пакетів даних на певному часовому відрізку приймає приблизно такий же самий вигляд після виконання масштабування, що при виконанні графічного відображення може приймати форму відповідного фракталу.

Взаємозв'язок між коефіцієнтом Херста та самоподібністю мережевого трафіку

Коефіцієнт Херста, H, у відношенні визначення самоподібності мережевого трафіку може визначати стан або відсутності властивості самоподібності або її наявності до певного ступеня.

Так, в загальному випадку, якщо коефіцієнт H приймає значення 0,5, то це вказує на те, що події є випадковими та між ними немає довгострокової залежності. В такому випадку мережевий трафік не є самоподібним.

Якщо коефіцієнт H приймає значення від 0,5 до 1, то це означає, що досліджуваний часовий відрізок представляє собою безперервну серію часу. Тобто чим більше значення приймає коефіцієнт H, тим більший ступінь довгострокової залежності між подіями та тим більший ступінь самоподібності. При значенні коефіцієнта Херста близького до 1 мережевий трафік приймає максимальне значення ступеня самоподібності, що означає, що при будь-якому масштабуванні часових рядів частота надходження пакетів даних буде приймати максимально схожий вигляд. В такому випадку, фрактальні властивості самоподібного процесу будуть відображені найбільш точно, а при графічному відображені мережевого трафіку з таким високим ступенем самоподібності будуть добре помітні фрактальні відображення частоти надходження пакетів даних.

Алгоритм визначення самоподібності мережевого трафіку

Для визначення коефіцієнта Херста розділимо тривалість надходження мережевого трафіку на фіксовані часові відрізки. Для опису часу надходження трафіку введемо часовий домен T, який розглядається як незалежна змінна для аналізу часових явищ. Отримані фіксовані часові відрізки X_i описуються за формулою $X = (X_i | i = 0,1,2,\ldots)$, де X – загальна тривалість моніторингу трафіку. Середнє значення частоти надходження пакетів позначимо через μ_t.

Для опису значення різниці максимальної та мінімальної частоти на кожному з часових відрізків визначимо функцію R(*T*), яка визначається за формулою [4]:

$$R(T) = \max X(t,T) - \min X(t,T), \text{ де } 1 \le t \le T$$

Для опису середнього відхилення частоти надходження пакетів даних від середнього значення частоти визначимо середнє квадратичне відхилення $S(T)$, яке визначається за формулою [4]:

$$S(T) = \{\frac{1}{T}\sum_{t=1}^{T}[X_t - \mu_t]^2\}^{\frac{1}{2}}, \quad (1)$$

де $X(t,T) = \sum_{i=1}^{t}[X_i - \mu_t]$

В такому випадку відношення $\frac{R(T)}{S(T)}$ приймає вигляд[4]:

$$\frac{R(T)}{S(T)} = cT^H \sim T^H, T \to \infty, \quad (2)$$

де H – коефіцієнт Херста;
c – константа.

Тоді коефіцієнт Херста обчислюється за формулою [4]:

$$\mathrm{H} = \frac{\ln(\frac{\mathrm{R}(T)}{\mathrm{S}(T)})}{\ln T} - \frac{\ln c}{\ln T} \tag{3}$$

В загальному випадку, для визначення ступеня самоподібності виконується обчислення значення функції $\mathrm{R}_i(n)$ та стандартного відхилення для кожного з часових відрізків довжиною *N*.

Далі для кожного з часових відрізків визначається відношення $\frac{\mathrm{R}_i(N)}{\mathrm{S}_i(N)}$ та обчислюється середнє значення $\frac{\mathrm{R}(N)}{\mathrm{S}(N)}$, при чому має виконуватись рівність [4]:

$$\frac{\mathrm{R}(N)}{\mathrm{S}(N)} = \frac{1}{k}\sum_{i=1}^{k}\frac{\mathrm{R}_i(N)}{\mathrm{S}_i(N)} \tag{4}$$

Також варто зазначити, що при збільшенні значення *N*, потрібно знову обчислювати відношення (4) та визначати коефіцієнт Херста за формулою (3), так як зміна кількості досліджуваних часових відрізків призводить до перерахунку значення коефіцієнта Херста, та, відповідно, до отримання нового значення ступеня самоподібності трафіку.

Постановка задачі

Завдяки особливостям повільних DoS-атак, які значно збільшують складність їх виявлення та великі загрози, які вони можуть спричинити, актуальною науково-практичною задачею є розроблення нових методів виявлення таких кібератак та проведення досліджень з метою визначення закономірностей їх мережевої поведінки. Виявлення DoS-атаки типу R.U.D.Y. здійснюється за допомогою аналізу мережевого трафіку, визначення його ступеня самоподібності та формування висновку щодо факту проведення атаки за допомогою методів машинного навчання.

Метод та програмні засоби виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку

В даній статті запропоновано метод виявлення DoS-атаки типу R.U.D.Y. за допомогою визначення ступеня самоподібності трафіку. Робота методу полягає у здійсненні аналізу мережевого трафіку, визначення ступеня самоподібності за допомогою коефіцієнта Херста та формування відповідного результату за допомогою використання апарату нейронних мереж.

В укрупненому варіанті представлення роботи алгоритму, метод складається з двох частин: навчання нейронної мережі попередньо отриманими даними про шкідливий трафік та виконання аналізу отримуваного мережевого трафіку для формування висновків щодо можливого виявлення кібератаки. При чому, для підвищення ефективності методу доцільно здійснювати виконання першої частини перед початком реального моніторингу мережевого трафіку, так як навчання нейронної мережі вимагає певного часу, протягом якого отриманий шкідливий трафік може бути проаналізований з недостатньою ефективністю. Укрупнена схема функціонування методу виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку зображена на рис. 1.

Рис. 1. Укрупнена схема функціонування методу виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку

У більш детальному варіанті представлення етап навчання складається з наступних кроків: збір вхідних даних для навчання з попередньо отриманого шкідливого трафіку, підготовка та нормалізація даних, навчання нейронної мережі. Етап виявлення складається з наступних кроків: збір даних з отримуваного мережевого трафіку, підготовка та нормалізація даних, визначення ступеня самоподібності. Загальна схема функціонування методу виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку зображена на рис. 2.

При використанні нейронної мережі для здійснення виявлення атаки використовується її здатність виявляти закономірності між вхідними та вихідними даними. Стосовно аналізу мережевого трафіку та визначення ступеня самоподібності, використання цієї властивості дозволяє виявляти шкідливий трафік на основі даних, які були відсутні при виконанні навчання. Іншими словами, використання нейронної мережі з алгоритмом визначення самоподібності дає можливість отримати вірний результат щодо стану системи на ранньому етапі виявлення.

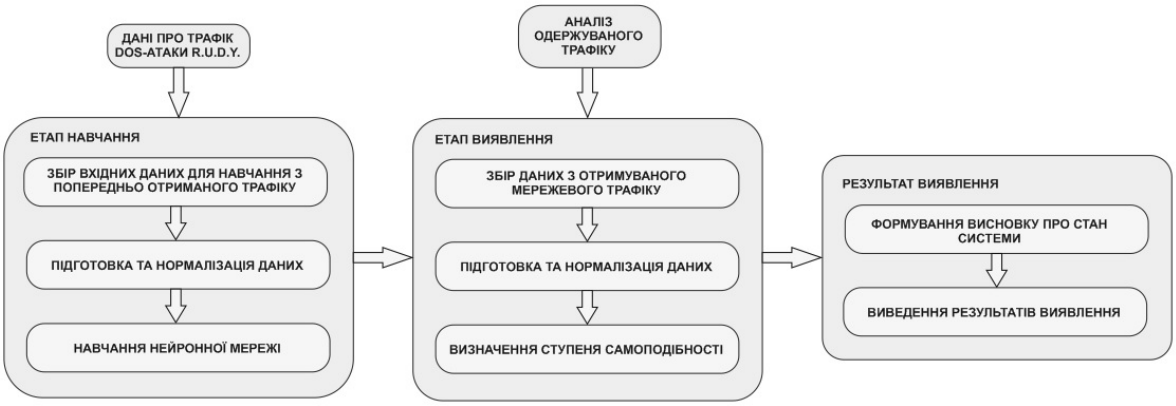

Рис. 2. Загальна схема функціонування методу виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку

Процес навчання нейронної мережі, її структура, вхідні та вихідні дані

Для здійснення розпізнавання зібраного мережевого трафіку використовується рекурентна нейронна мережа. В основі методу розпізнавання мережевого трафіку нейронною мережею лежить алгоритм визначення самоподібності трафіку. Процес навчання нейронної мережі полягає у здійсненні аналізу попередньо зібраного трафіку атаки R.U.D.Y. та визначенні відношення між ступенями самоподібності на різних часових відрізках між попередньо зібраним трафіком атаки R.U.D.Y. та отриманим відфільтрованим мережевим трафіком. Набір значень та кількість часових відрізків визначаються при виконанні розподілу загального часового ряду. Такий розподіл часового ряду, який відображає кількість та частоту отриманих пакетів даних можна реалізувати за допомогою розбиття загального ряду на N однакових інтервалів. В такому випадку, необхідна кількість часових відрізків для здійснення максимально ефективного виявлення атаки визначається експериментальним шляхом. Використання такого розподілу дозволяє відобразити властивість масштабованості, яка характерна самоподібним процесам.

Під час аналізу отримуваного трафіку для виявлення атаки, важливою перевагою рекурентної нейронної мережі є її висока ефективність обробки серій подій у часі. Так як кількість часових відрізків та кількість зібраних пакетів на даних відрізках може бути різна, то зручною виявляється властивість рекурентних нейронних мереж використовувати свою внутрішню пам’ять для обробки послідовностей довільної довжини.

Одним із недоліків рекурентних нейронних мереж є необхідність створення для кожного досліджуваного дискретного інтервалу часу свого шару нейронів, що може збільшувати загальну обчислювальну складність розроблюваної системи. Також варто зазначити, що атака R.U.D.Y. спроектована таким чином, що після створення певної кількості підключень до сервера, кожен з потоків зазвичай здійснює відправку пакетів з приблизно однаковою частотою. Тому, для забезпечення можливості здійснення аналізу отримуваного трафіку у режимі реального часу використовується механізм накопичення пакетів до певної мінімальної величини, k.

Величиною k, можна вважати ту кількість отриманих пакетів, яка лежить між кількістю IP-пакетів, які створює атака R.U.D.Y., що фактично можуть спричинити DoS-стан атакованої комп’ютерної системи та між мінімальним значенням кількості пакетів, величина якого достатня для отримання достовірного значення ступеня самоподібності. В такому випадку, наступним моментом мінімального досліджуваного інтервалу часу можна вважати момент здійснення даного накопичення.

Структура використовуваної рекурентної нейронної мережі зображена на рис. 3.

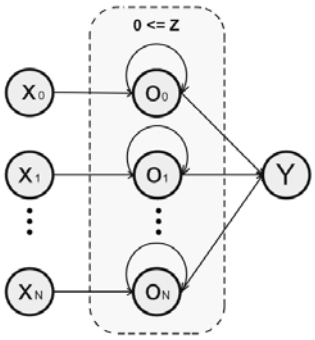

Рис. 3. Структура нейронної мережі

Як показано на рис. 3, кількість нейронів вхідного шару та кількість елементів у внутрішньому шарі дорівнює кількості часових відрізків N.

Використовувану рекурентну нейронну мережу можна представити у вигляді сукупності

розгорнутих у часі нейронних мереж з прямим розповсюдженням сигналу. В такому випадку кожен з елементів $O_0 \dots O_N$, які показані на рис. 3 можна представити у розгорнутому вигляді, як зображено на рис. 4.

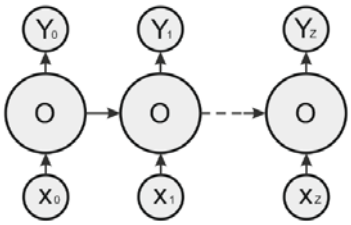

Рис. 4. Структура внутрішніх нейронів, розгорнутих у часі

Як показано на рис. 4, кількість внутрішніх розгорток дорівнює змінній *Z*, величина якої залежить від мінімальної довжини інтервалу, *k*, таким чином, що послідовний розподіл загального часового ряду *T*, відбувається розбиттям на *N* відрізків, після чого отримані нові часові відрізки, також діляться на *N* частин, поки довжина останнього відрізку не буде менша довжини відрізку з *k* пакетів. Значення *Z* дорівнює кількості ітерацій процедури розбиття часових відрізків.

За характером навчання використовувана нейронна мережа належить до класу навчання з учителем. Для здійснення навчання використовується алгоритм зворотного поширення помилки. Завдяки наявності попередньо зібраного трафіку атаки R.U.D.Y., стають відомі правильні відповіді, які нейронна мережа повинна згенерувати на останньому етапі роботи. При отриманні помилкової відповіді на кінцевому шарі мережі, визначається значення помилки на усіх попередніх шарах.

Перед початком навчання нейронної мережі та при отриманні мережевих пакетів виконується попередня підготовка та нормалізація даних. Такі початкові вхідні дані складаються з мережевого трафіку, який представлений у вигляді множини POST HTTP запитів, та відповідної послідовності отриманих IP-пакетів, які отримуються під час надсилання даних при здійсненні атаки. При чому, для ідентифікації мережевих потоків і подальшого виявлення атаки здійснюється аналіз лише тих частин заголовків HTTP-запитів та IP-пакетів, значення яких потрібні для виявлення атаки. В такому випадку, кожен отриманий POST HTTP запит можна представити у вигляді кортежу:

$$X_1 = (\textbf{Content-Length, Connection}),$$

де **Content-Length** – розмір даних у байтах. Великі значення **Content-Length** свідчать про потенційно небезпечний трафік, характерний для кібератаки R.U.D.Y. Зчитування та аналіз даного поля заголовка дозволяє ідентифікувати та ізолювати шкідливий потік даних поміж звичайних потоків;

Connetction – відомості про стан підключення. Моніторинг статусу підключення потоків дозволяє визначати початок та закінчення передачі пакетів даних з конкретної IP-адреси.

Кожен з отриманих IP-пакетів можна представити у вигляді кортежу:

$$X_2 = (\textbf{Size, Source, Time}),$$

де **Size** – розмір IP-пакету, включаючи заголовок та дані. Подібні розміри IP-пакетів, які були отримані з певного POST HTTP запиту, та які відправлялися з низькою частотою також свідчать про небезпечний трафік, характерний для атаки R.U.D.Y.;

Source – IP-адреса відправника пакета. Визначення IP-адрес дозволяє ідентифікувати IP-адресу комп'ютера зловмисника;

Time – час отримання IP-пакету. Перед початком визначення ступеня самоподібності множина значень часу надходження IP-пакетів дає можливість створити графік надходження пакетів на відповідних часових відрізках та сформувати вхідні дані для нейронної мережі.

На етапі навчання нейронної мережі попередньо зібраний трафік атаки R.U.D.Y. зберігається у вигляді набору бінарних файлів, кожен з яких представляє трафік з певною, наперед визначеною кількістю підключень до сервера. Вхідні дані, які записані в цих файлах, зберігаються у вигляді послідовності записів, кожен з яких можна представити у вигляді кортежу:

$$(X_1,\ X_{2_1} \dots X_{2_N}),$$

де X_1 – кортеж, який описує POST HTTP підключення;

$X_{2_1} \dots X_{2_N}$ – набір кортежів, які описують отримані IP-пакети;

N – загальна кількість IP-пакетів.

На етапі аналізу нейронною мережею отримуваного трафіку, дані про трафік представляються у вигляді наборів кортежів типу X_1 та X_2 у невизначеному порядку, так як до сервера може бути здійснено безліч різних POST HTTP запитів, кожен з яких буди містити в собі пакети даних у невизначеній кількості, які будуть відправлятися у різні моменти часу. В такому випадку, для ідентифікації певного POST HTTP запиту з відправником цього запиту, використовується механізм зчитування адреси та номера порта сокета

відправника даних. Це дозволяє визначити спільне джерело отримання POST HTTP запитів, а для визначення приналежності між множиною отриманих IP-пакетів та відповідним POST HTTP запитом, виконується зчитування даних сокетом з заданим буфером достатнього розміру, що дозволяє одночасно зчитувати заголовки POST HTTP запитів та IP-пакетів.

Підготовка даних для нейронної мережі полягає у створенні вектора нормалізованих даних для нейронів вхідного шару на основі множини кортежів типу X_2. Такі вектори складаються з наборів цілих чисел, кожне з яких означає кількість отриманих IP-пакетів на певному конкретному моменті часу. При чому мінімальною дискретною одиницею часу вважається 1 мс.. Вихідними значеннями нейронів внутрішніх шарів є значення ступеня самоподібності при заданих вхідних векторах на різних часових інтервалах та підінтервалах. Значенням вихідного шару, який складається з одного нейрону, є число, яке визначає ступінь схожості проаналізованого мережевого трафіку з попередньо зібраним трафіком DoS-атаки R.U.D.Y.

Експерименти

Для оцінки ефективності запропонованого методу виявлення кібератаки типу R.U.D.Y. було проведено ряд експериментів. Для здійснення можливості проведення таких експериментів та побудови відповідного експериментального середовища зручно використовувати програмні засоби віртуалізації, такі як, наприклад, VirtualBox.

Використовуване експериментальне середовище зображене на рис. 5.

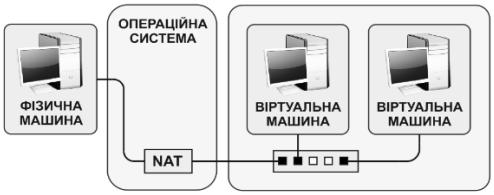

Рис. 5. Експериментальне середовище

Як показано на рис. 5, експериментальне середовище складається з комп'ютера-хоста, який представляє собою фізичну машину та двох віртуальних машин. При чому, одна з віртуальних машин виконує роль нападника, а інша машина – роль веб-сервера, на який планується здійснення DoS-атаки.

Для виконання експериментів була здійснена атака на віртуальний веб-сервер Apache з віртуальної машини нападника. Основними параметрами DoS-атаки R.U.D.Y. є кількість мережевих підключень до сервера, на який планується здійснення атаки; значення поля Content-Length відповідних POST HTTP запитів та частота відправки пакетів з кожного відкритого підключення. Також, для здійснення атаки потрібно вказати URL веб-сервера. Для виконання експериментів був використаний URL http://192.168.1.1, що представляє собою локальну IP-адресу віртуальної машини веб-сервера. Для віртуальної машини нападника була призначена IP-адреса 192.168.1.2. Параметри DoS-атаки R.U.D.Y., які використовувались для проведення експериментів представлені у таблиці 1.

Таблиця 1

Параметри DoS-атаки R.U.D.Y. для проведення експериментів

Параметр атаки R.U.D.Y.	Значення параметра атаки R.U.D.Y.
Кількість підключень	50
Значення Content-Length	100000000
Частота відправки пакетів	1 с

Використаний у роботі алгоритм визначення самоподібності трафіку може бути протестований за допомогою зміни вхідних значень та порівняння відповідних отриманих вихідних результатів. Параметри алгоритму визначення самоподібності трафіку, які були використані під час виконання експерименту, представлені у таблиці 2.

Таблиця 2

Параметри алгоритму визначення самоподібності трафіку

Параметр алгоритму	Значення параметра алгоритму
Загальна величина часового ряду, T	10 с
Кількість часових відрізків, i	12
Кількість пакетів даних на кожному з часових відрізків, $k_1 \ldots k_i$	~50

Можливі результати визначення коефіцієнта Херста на кожному з часових відрізків зображені на рис. 6.

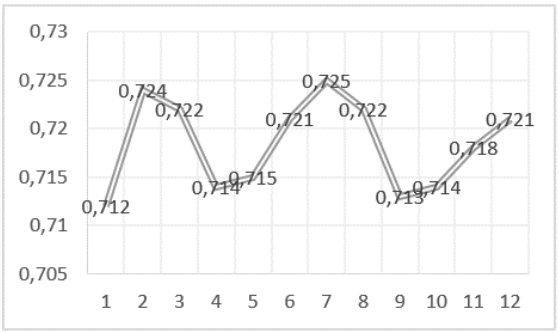

Рис. 6. Результати визначення коефіцієнта Херста

Як показано на рис. 6, коефіцієнт Херста в загальному приймає значення близько 0,7, що свідчить про те, що протестований трафік є частково самоподібним.

Таким чином, запропонований метод виявлення може бути основою для побудови програмного забезпечення систем виявлення DoS-атак типу R.U.D.Y.

Висновки

В даній статті описано метод виявлення DoS-атаки типу R.U.D.Y. за допомогою алгоритму визначення самоподібності мережевого трафіку. Описаний метод дає можливість виявляти шкідливі потоки пакетів даних серед звичайних, а постійний моніторинг визначених шкідливих потоків дає можливість виявити зловмисника та дозволяє ізолювати звичайний мережевий потік даних від шкідливого.

Література

1. R. Matherw, V. Katkar. Survey of Low Rate DoS Attack Detection Mechanisms. International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India. P. 955–958.

2. W.E. Leland, M.S. Taqqu, W. Willinger, D.V. Wilson. On the Self-Similar Nature of Ethernet Traffic. (Originally Published in: Proc. SIGCOMM ’93, Vol. 23, No. 4, October 1993). P. 202–213.

3. Will E. Leland, Murad S. Taqqu, Walter Willinger, Daniel V. Wilson. On the Self-Similar Nature of Ethernet Traffic (Extended Version). IEEE/ACM Transactions on Networking, Vol. 2, No. 1, February 1994.

4. Zhang Sheng, Zhang Qifei, Pan Xuezeng, Zhu Xuhui. Detection of Low-rate DDoS-Attack Based on Self-Similarity. 2010 Second International Workshop on Education Technology and Computer Science. P. 333–336.

5. Walter Willinger, Murad S. Taqqu, Robert Sherman, Daniel V. Wilson. Self-Similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level. IEEE/ACM Transactions on Networking, Vol. 5, No. 1, February 1997. P. 71–86.

6. Walter Willinger, Murad S. Taqqu, Will E. Leland, Daniel V. Willson. Self-Similarity in High-Speed Packet Traffic: Analysis and Modeling of Ethernet Traffic Measurments. Statistical Sciencem 1995, Vol. 10, No. 1, P. 67–85.

7. Maryam M. Najafabadi, Taghi M. Khoshgoftaar, Amri Napolitano, Charles Wheelus. RUDY Attack. Detection at the Network Level and Its Important Features. Proceedings of the Twenty-Ninth International Florida Artificial Intelligence Research Society Conference. P. 282–287.

8. Payal Jain, Juhi Jain, Zatin Gupta. Mitigation of Denial of Service (DoS) Attack. IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 201, ISSN (Online): 2230-7893, www.IJCEM.org. P. 38–44.

9. Junhan Park, Keisuke Iwai, Hidema Tanaka and Takakazu Kurokawa. Analysis of Slow Read DoS attack. ISITA2014, Melbourne, Australlia, October 26–29, 2014. P. 60–64.

10. Gabriel Macia-Fernandez, Jesus E. Dıaz-Verdejo, Pedro Garcıa-Teodoro. Evaluation of a low-rate DoS attack against application servers. Department of Signal Theory, Telematics and Communications, E.T.S. Computer and Telecommunications Engineering, University of Granada, c/ Danielo Aranda, s/n 18071 Granada, Spain. Computers & Security 27 (2008). P. 335–354.

11. Evan Damon, Julian Dale, Evaristo Laron, Jens Mache, Nathan Land, Richard Weiss. Hands-On Denial of Service Lab Exercises Using Slowloris and RUDY. P. 21–29.

Рецензія/Peer review : 21.5.2019 р. Надрукована/Printed : 2.6.2019 р.
Рецензент: д.т.н., проф. Говорущенко Т.О.