DOI 10.31891/2307-5732-2020-281-1-156-163
УДК 621.391 160164

А.О. НІЧЕПОРУК, А.А. НІЧЕПОРУК, О.В. ФЕГИР, А.Д. КАЗАНЦЕВ, Ю.О. НІЧЕПОРУК
Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ DDOS АТАК НА ІОТ МЕРЕЖІ

В роботі представлено метод виявлення DDoS атак на IoT-мережі, що заснований на використанні логістичної регресії. Запропонований метод складається з двох етапів: offline та online. Головною метою offline етапу є створення моделі класифікатора, яка буде в подальшому використана в процесі виконання online етапу. Шляхом моніторингу мережевого трафіку в режимі реального часу етап online здійснює виявлення DDoS атак на основі використання сформованої на етапі offline моделі класифікатора. Процес виявлення передбачає розбиття спостережуваного періоду моніторингу трафіку на 10 відрізків та визначення на кожному з них проміжних результатів. Висновок про наявність DDoS атаки здійснюється на основі порівняння середнього значення серед всіх проміжних результатів класифікації з пороговим значенням виявлення. У випадку перевищення порогового значення робиться висновок про наявність DDoS атаки.

Ключові слова:DDoS атака, IoT, класифікатор, мережевий трафік

A.O.NICHEPORUK, A.A. NICHEPORUK, O.V. FEHYR, A.D. KAZANTSEV, Y.O. NICHEPORUK
Khmelnytskyi National University

METHOD OF DETECTING DDOS ATTACKS ON IOT NETWORKS

The paper presents a method for detecting DDoS attacks on an IoT network based on the use of logistic regression. With limited computing power and available memory on IoT networks, the use of logistic regression is dictated by the low computational complexity and ease of implementation. The proposed method consists of two steps: offline and online. The main purpose of the offline stage is to create a classifier model that will be further used in the online stage execution process. The main purpose of the offline stage is that in during training the logistic classifier model, the entire training data set is split into two sets. The first dataset is labeled and will be used to train the logistic regression classifier. The second dataset is also labeled and used for validation. The training algorithm does not use validation dataset labels, instead they are used to test the predicted output of the classifier.

By monitoring network traffic in real time, the online stage detects DDoS attacks based on the use of the offline classifier model. The detection process involves splitting the monitored monitoring period into 10 segments and identifying intermediate results on each of them. The conclusion that a DDoS attack is present is based on a comparison of the mean among all the intermediate classification results with the detection threshold. If the threshold is exceeded, it is concluded that a DDoS attack is present.

According to the results of a study using the developed software, the highest efficiency of DDoS detection of TCP SYN attacks was achieved at the level of 91%. However, with the highest detection efficiency, the type 1 error rate was also the highest, at 10%. After carrying out 10 experiments, the average values of statistical indicators were determined, in particular the accuracy value was 89.9%, and the level of false positives was 9.6%.

Keywords: DDoS attack, IoT, classifier, network traffic

Вступ

Зростаюча популярність IoT (або “інтернет речей”) надає широкі можливості для покращення, планування та автоматизації нашого життя. IoT дозволяє поєднувати в мережу та керувати множиною пристроїв, які забезпечують збір, аналіз та передачу даних. Сфера застосування IoT з кожним роком продовжує розширюватися, охоплюючи нові сфери життя, починаючи від розумних будинків, міст та закінчуючи сферою охорони здоров’я.

Проте разом із очевидними перевагами та зручностями, що несе із собою використання IoT, концепція “інтернет речей” залишає для зловмисників ряд потенційних “вузьких”місць у безпеці таких систем. Персональні дані, зібрані IoT-пристроями, завжди мають цінність для хакерів і викрадачів конфеденційної інформації. Крім того, кібератака на IoT-рішення потенційно здатна завдати шкоди фізичним сервісам та фізичній інфраструктурі.

Згідно з доповіддю Arbor Security [1], атаки DDoS на IoT системи були найбільш домінуючим видом атаки у 2017 році, а 65% всіх атак, виявлених у 2016 році, були об’ємною атакою DDoS. Атака Mirai DDoS [2], яка є найбільш масовою DDoS атакою, була здійснена шляхом інфікування незахищених пристроїв IoT. На сьогоднішній день найпоширенішими DDoS-атаками є TCP, UDP, SYN та DNS атаки. Через обмеження в пам’яті, обробці, енергетичних обмеженнях та неоднорідному характері пристроїв IoT реалізація систем захисту та безпеки в таких пристроях є складною та актуальною проблемою.

Попередні дослідження

На сьогоднішній день проблемі виявлення вторгнень в IoT мережі присвячується значена увага. Серед основних напрямків по виявленню DDoS атак можна відзначити використання ентропійного аналізу, визначення належності досліджуваного трафіку до одного із законів розподілу випадкових величин, залучення систем на основі правил, використання методів машинного навчання, обчислення та порівняння статистичних величин, наприклад, кількості пакетів, часу затримки між пакетами, кількість одиничних пакетів, протокол передачі, тощо. Розглянемо детальніше відомі підходи до виявлення DDoS атак у IoT мережах.

У роботі [3] було запропоновано алгоритм захисту IoT мереж перед DDoS-атакам, шляхом надання IoT пристроям інтелектуальних можливостей, подібних до ботів. Щоб зрозуміти різницю між доброякісним

і шкідливим запитом, вузол здійснює аналіз вмісту пакету. Хоча результати показали, що такий підхід допомагає запобігти атакам, проте продуктивність роботи методу сильно залежить від обмежених ресурсів кожного бота.

Хостова система на основі виявлення та запобігання вторгнень (IoT-IDM) у IoT мережах представлена у роботі [4]. Система IoT-IDM відстежує зловмисну активність та блокує доступ до пристроїв за допомогою програмно визначених програмних мереж (SDN) з використанням протоколу OpenFlow. Після того, як атака в оточенні SmartHome виявлена на рівні мережі, IoT-IDM створює політику для блокування та переміщення інфікованих хостів у карантин. Проте слід відзначити, що оцінка роботи IoT-IDM проводилася лише за допомогою сценарію атаки проти smart ламп. Окрім того, система IoT-IDM має обмежені можливості для додавання нових пристроїв у ручному режим, що ускладнює користувачам роботу з нею.

На відміну від системи IoT-IDM та його аналізу пакетів, автори роботи [5] змінили вихідний код з IoT ботнета Mirai та розгорнули доброякісний ботнет. Цей ботнет використовує ту саму компрометуючу техніку для сканування та створення списку вразливих пристроїв та служб протидії інфікуванню, які залучаються при виявлені вразливості. Для уникнення подальшого інфікування та запобіганню подальшому поширенню з вихідного коду, що розроблявся для атаки на сервери telnet, SSH та HTTP, було видалено всі зловмисні функції. Незважаючи на те, що всі функції атаки були видалені та враховуючи технічну доцільність такої стратегії, автор визнає, що підхід порушує закони у багатьох юрисдикціях, враховуючи відсутність географічних меж таких ботнетів.

У роботі [6] авторами запропоновану систему виявлення вторгнень (IDS) на основі обробки подій для IoT. Ця система заснована на специфікаціях та використовує методи оброблення події для виявлення атак. Запропонована система збирає дані з пристроїв IoT, отримує список подій та виконує виявлення DDoS атак шляхом зіставлення списку подій із наборами правил, що зберігаються в сховищі правил.

У роботі [7] запропоновано алгоритм виявлення DDoS атак на основі використання інформаційних метрик. Авторами представлено два статистичні показники, узагальнену ентропію та інформаційну відстань для виявлення швидкоплинних DDoS-атак. В основі представленої роботи робиться припущення про різний розподіл мережевого трафіку. Так у випадку відсутності DDoS атаки розподіл трафіку підкорюється Гаусівському закону, тоді як під час атаки розподіл мережевого трафіку – закону Пуассона. Рішення про інфікування приймається на основі різниці в інформаційних показниках між легітимним та шкідливим трафіком.

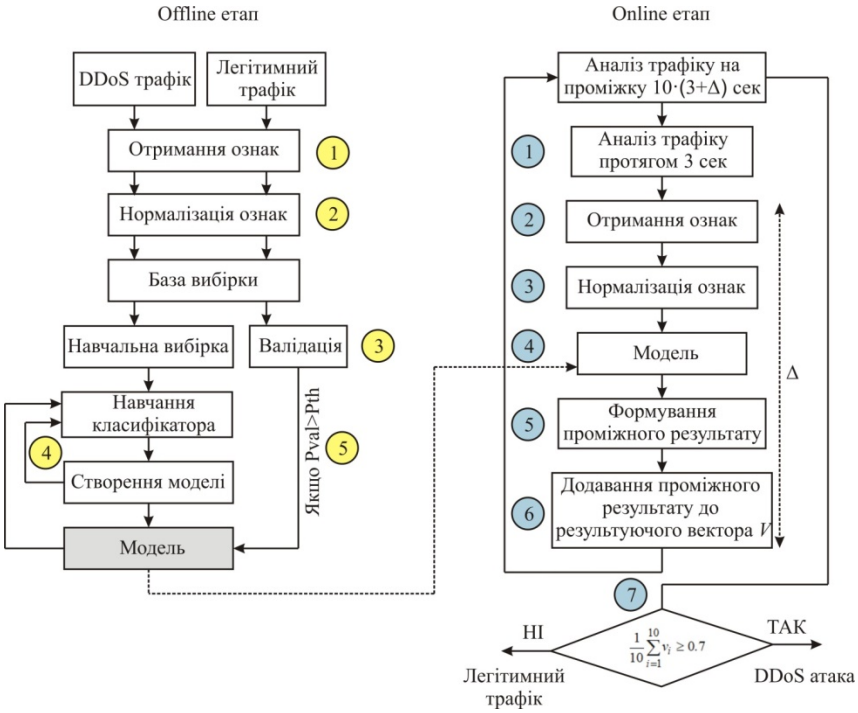

Рис. 1. Узагальнена схема методу виявлення DDoS атак на IoT-мережі

Ще один підхід заснований на обчисленні ентропії представлений у роботі [8]. Автори розробили IDS систему, що заснована на зміні розмірів пакетів ентропії інформації при DDoS атаці на IoT мережу. Результати їх експериментів, що представлений підхід здатний здійснити виявлення як короткочасних, так і довгострокових атак.

Підхід, який для виявлення бот-мереж в IoT залучає штучну нейронну мережу, що використовується для навчання ефективних кодувань, представлено у роботі [9]. В основі підходу лежить принцип навчання нейронної мережі для кожного IoT вузла в мережі. В результаті множини експериментів авторами було продемонстровано високий рівень ефективності виявлення із незначним рівнем хибних спрацювань. Однак завдяки навчанню автокодувальника для кожного пристрою обчислювальна складність

запропонованого методу є високою, що унеможливлює його масштабування та розгортання в існуючих IoT мережах.

Метод виявлення DDoS атак на IoT мережі

З метою підвищення ефективності виявлення DDoS атак у мережах інтернету речей запропоновано метод на основі використання логічтисного класифікатора, що складається з двох етапів: offline та online. Узагальнену схему методу виявлення DDoS атак на IoT-мережі наведено на рис. 1. Розглянемо детальніше кроки запропонованого методу.

Класифікатор на основі логістичної регресії

В якості класифікатора, що використовується у запропонованому методі виявлення DDoS атак на IoT-мережі використано метод логістичної регресії.

Метод логістичної регресії визначає взаємозв'язок між категоріально залежною змінною та однією або кількома незалежними змінними шляхом оцінки ймовірностей за допомогою логістичної функції. Незалежні змінні $X = \{x_1, x_2, ..., x_n\}$ – це ознаки або вхідні дані, які будуть використовуватись для прогнозування цілі, залежною змінною є змінна класу цілі або вихідні дані *Y*, які необхідно передбачити зі значеннями 0 або 1. Тобто класифікатор на основі логістичної регресії здійснює визначення імовірності *P* належності вхідного об'єкта *X*, що заданий множиною незалежних змінних $x_1, x_2, ..., x_n$, до одного із класів, тобто *Y=C,* де значення *C* приймає 0 або 1. В нашому дослідженні значенню 1 відповідатиме наявність підозрілої активності у мережевому трафіку, що свідчить про DDoS атаку. Натомість значенню 0 відповідає категорія легітимний трафік, в якому відсутні ознаки DDoS атаки. У випадку бінарного класифікатора K , рішення про віднесення досліджуваного об'єкта до одного із класів приймається в залежності від порогового значення φ:

$$\mathrm{K} = \begin{cases} Y = 1, if\ P \geq \varphi, \\ Y = 0, if\ P < \varphi, \end{cases} \tag{1}$$

В основі класифікатора застосовується сигмоїдна функція:

$$f(x) = \frac{1}{1 + e^{-Z}} \tag{2}$$

Тоді для обчислення імовірності належності вхідного об'єкта *X*, до класу, що визначає наявність DDoS атаки визначається як:

$$P(Y = 1 \mid X) = \frac{1}{1 + e^{-Z}} \tag{3}$$

Аналогічним чином, беручи до уваги, що змінна *Y*, приймає тільки два значення 0 та 1, імовірність належності об'єкта *X*, до класу, що відповідає легітимному трафіку визначається як:

$$P(Y = 0 \mid X) = 1 - P(Y = 1 \mid X) \tag{4}$$

де у виразах 3.3 та 3.4 значення *Z* обчислюється як:

$$Z = \theta^T X = \theta_0 + \theta_1 x_1 + \theta_2 x_2 + ... + \theta_n x_n \tag{5}$$

де $x_1, x_2, ..., x_n$ *n* ознак, що надходять на вхід до класифікатора, $\theta_1, \theta_2, ..., \theta_n$ коефіцієнти регресії.

Для навчання або підбору параметрів $\theta_1, \theta_2, ..., \theta_n$ необхідно скласти навчальну вибірку, що складається із наборів значень незалежних змінних та відповідних їх значень залежної змінної. Формально, це множина пар $(x^{(1)}, y^{(1)}), ..., (x^{(m)}, y^{(m)})$, де $x^{(i)} \in R^n$ – вектор значень незалежних змінних, а $y^{(i)} \in \{0,1\}$ – відповідне їм значення *y*. Кожна така пара називається навчаючим прикладом.

Для навчання класифікатора на основі логістичної регресії використовується метод максимальної правдоподібності, згідно із яким вибираються параметри θ_i, що максимізують значення функції правдоподібності на навчальній вибірці:

$$\hat{\theta} = arg\ max_\theta\ L(\theta) = arg\ max_\theta \prod_{i=1}^{m} P\{ y = y^i \mid x = x^i \} \tag{6}$$

Оскільки максимізація функції правдоподібності еквівалента максимізації її логарифму, то можна записати вираз 3.6 наступним чином:

$$log\ L(\theta) = \sum_{i=1}^{m} log\ P\{ y = y^i \mid x = x^i \} \tag{7}$$

Для максимізації цієї функції може бути застосований, наприклад, метод градієнтного спуску. Він полягає у виконанні наступних ітерацій, починаючи з деякого початкового значення параметрів θ_i:

$$\theta := \theta + \alpha \nabla\ log\ L(\theta) = \theta + \alpha \sum_{i=1}^{m} (y^{(i)} - f(\theta^T x^{(i)})) x^{(i)}, \alpha > 0 \tag{8}$$

Offline етап

Головною метою Offline етапу є створення моделі класифікатора, яка буде в подальшому використана в процесі виконання Online етапу. Наведемо кроки offline етапу для методу виявлення DDoS атак на IoT-мережі (рис.1):

На основі множини зразків легітимного та DDoS трафіку отримання ознак, на основі яких здійснюватиметься навчання моделі класифікатора.

Нормалізації отриманих ознак та приведення їх значення до дійсних чисел в діапазоні від 0 до 1. Отримання бази вибірки.

Розбиття бази вибірки на дві частини у співвідношенні 80% до 20%, тобто навчальну вибірку та вибірку для валідації відповідно.

Навчання класифікатора.

Виконання навчання класифікатора на множині тестових даних.

Перевірка створеної моделі класифікатора на даних для валідації. Якщо імовірність належності значення прикладу із даних для валідації до одного із класів більша за 0,9, то включення цього прикладу до моделі.

Розглянемо детальніше кроки Offline етапу.

Розмежування поведінки між легітимним та DDoS трафіком здійснюється на основі аналізу пакетів, які функціонують у IoT-мережі. В процесі моніторингу мережевого трафіку здійснюється відбір ознак із пакетів, що дозволяють ідентифікувати DDoS атаку. В запропонованому методі цими ознаками є: розмір пакету, часовий інтервал надходження пакетів, різниця між розміром пакетів, тип протоколу та IP адреса призначення.

Всі значення ознак отримуються з pcap файлів із використанням утиліти wireshark та NetworkTrafficView.

Таким чином для кожного екземпляру легітимного та DDoS IoT-трафіку, що представлений у .pcap файлі буде отримано вектор ознак у форматі CSV (comma separated vector):

$$X = \left\langle x_{ps}, x_{\Delta t}, x_{\Delta s}, x_{pr}, x_{ip} \right\rangle \tag{9}$$

Всі вектори ознак були згруповані у два файли: один для легітимного трафіку, інший для DDoS трафіку.

З метою приведення різнорідних даних до чисел в діапазоні дійсних чисел від 0 до 1 наступним кроком є нормалізація значень векторів ознак з використанням мін-макс нормалізації:

$$x' = \frac{x - min\, x}{max\, x - min\, x}, \tag{10}$$

де x' – нормалізоване значення ознаки, $min\, x$ та $max\, x$ – мінімальне та максимальне значення ознаки x у навчальній вибірці відповідно.

Наступним кроком offline етапу є розбиття бази вибірки на дві частини у співвідношенні 80% до 20%. Перший набір даних є маркованим, і він буде використовуватися для тренування класифікатора на основі логістичної регресії. Він був позначений як навчальний набір даних. Другий набір даних також є маркованим і використовується для валідації, ми позначили його як набір даних для валідації. Алгоритм навчання не використовує мітки набору даних валідації, натомість мітки використовуються для перевірки передбачуваного виходу класифікатора.

Запропонована система виявлення для класифікатора на основі логістичної регресії використовує напівавтоматичний алгоритм машинного навчання.

Етап навчання складається з двох кроків. На першому кроці етапу навчання навчальний набір даних, завантажується в алгоритм навчання. Кожен рядок навчального набору даних є навчальним прикладом з шістьох ознак $\left\langle x_{ps}, x_{\Delta t}, x_{\Delta s}, x_{pr}, x_{ip} \right\rangle$ та мітки (Y). Мітка приймає значення або 1, або 0 (DDoS атака або легітимний трафік).

За допомогою навчального набору даних алгоритм тренування здійснює обчислення набору коефіцієнтів θ_i із залученням методу найбільшої правдоподібності (3.7, 3.8).

На другому кроці коефіцієнти, що отримані на першому кроці, підставляються у вираз 3.5 для обчислення значення Z для кожного навчального прикладу з набору даних валідації. Після визначення значення Z виконуємо обчислення логістичної функції, і таким чином, ймовірності того, що навчальний приклад належить до класу 1 та 0, використовуючи рівняння 3.3 та 3.4 відповідно. Таким чином дані, з розміченого набору даних, що мають високий ступінь належності до одного із класів будуть додані до початкового тестового набору для підвищення ефективності роботи класифікатор.

Розмічені дані включаються у навчальну вибірку, якщо їх ступінь належності до одного із класів C більший за значення P_{th}:

$$P(Y = C \mid X) \geq P_{th} \tag{11}$$

Значення P_{th} є пороговим значенням імовірності включення навчального прикладу до навчальної моделі класифікатора. Навчальні приклади, що продемонстрували низький ступінь довіри, не будуть додані до навчального набору даних.

Online етап

Етап online здійснюється для безпосереднього виявлення DDoS атак в мережах Інтернету речей та передбачає виконання наступних кроків:

Аналіз мережевого трафіку на протязі 3 сек;

Отримання ознак;

Нормалізації отриманих ознак та приведення їх значення до дійсних чисел в діапазоні від 0 до 1;

Використовуючи модель класифікатора, що була створена на етапі offline, виконання класифікації мережевого трафіку;

Формування проміжного результату;

Додавання проміжного результату класифікації до результуючого вектора *V*.

Повторення кроків 1-6 десять разів;

На основі десяти значень результатів класифікації визначення результуючого результату про наявність DDoS атаки.

Розглянемо детальне кроки online етапу для методу виявлення DDoS атак в IoT-мережах.

Першим кроком online методу є моніторинг мережевого трафіку на протязі визначеного часового інтервалу. Визначення часового інтервалу для збору записів із мережевого трафіку має велике значення. Якщо збір проводиться через тривалі інтервали, то буде значна затримка для виявлення нападу і, як наслідок, скорочення часу, необхідного для блокування DDoS атаки. З іншого боку, якщо інтервал часу для моніторингу буде занадто коротким, відбудеться збільшення накладних витрат на збір та опрацювання ознак. У нашому дослідженні в якості часового інтервалу, на протязі якого здійснюється моніторинг трафіку, було обрано 3 сек.

Другий та третій крок online етапу, що передбачають отримання ознак та їх нормалізація аналогічні першому та другому кроку offline етапу методу виявлення DDoS атак в IoT-мережах.

Наступний крок online етапу передбачає використання моделі класифікатора, що був створений на етапі online. З цією метою здійснюється залучення логістичної функції, у яку підставляються значення отриманих ознак з мережевого трафіку, що отримані на другому та третьому кроці методу. Слід відзначити, що значення коефіцієнтів θ_i отримуються в процесі навчання класифікатора на етапі offline. В результаті висновок про наявність DDoS атаки здійснюється на основі використання формули 1. Значення коефіцієнта φ було обрано на рівні 0,5. Тобто, висновок про наявність DDoS атаки приймається, якщо значення імовірності, що обчислене в результаті підстановки ознак у логістичну функцію буде більше або дорівнювати значенню 0,5. У такому випадку значення проміжного результату складе $v_j = 1$, де $j = \overline{1,10}$. В іншому випадку значення $v_j = 0$. Визначене таким чином значення часткового результату додається до результуючого вектора *V*.

Для визначення остаточного результату про наявність DDoS атаки на IoT- мережу здійснюється визначення середнього арифметичного для всіх проміжних результатів класифікації та порівняння із пороговим значенням рівня виявлення:

$$\frac{1}{10}\sum_{j=1}^{10} v_j \geq 0.7 \qquad (12)$$

Таким чином online етап виявлення DDoS атак передбачає моніторинг мережевого трафіку на проміжку $10 \cdot (3 + \Delta)$ сек, тобто розбиття спостережуваного періоду моніторингу на 10 відрізків та визначення на кожному з них проміжних результатів. Слід відзначити, що час моніторингу на кожному відрізку визначається сумою часу безпосереднього моніторингу та часу, що витрачається на отримання ознак, нормалізацію та класифікацію. На кожному з відрізків час моніторингу складає 3 сек.

Експерименти

Для проведення експериментальних досліджень по перевірці ефективності запропоновано методу виявлення DDoS-атаки необхідним завданням є генерація легітимного та DDoS мережевого трафік. Спочатку було згенервано DDoS та легітимний трафік окремо, а потім дві множин трафіку були поєднанні разом в одну навчальну вибірку.

Отримання DDoS-трафіку

Для створення DDoS-трафіку було використано дві комп'ютерні системи з операційною системою Kali Linux, що працюють у віртуальному середовищі Oracle VirtualBox, одна з яких виступала цільовою платформою для DDoS атаки, а інша – комп'ютерна система. Обидві комп'ютерні системи були підключені до однієї мережі Wi-Fi. Мережевий трафік на машині жертви збирався за допомогою утиліти Wireshark. Потоки TCP SYN і UDP flood були згенеровані за допомогою утиліти hping3, що входить до операційної системи Kali Linux. Вигляд запуску команди генерування DDoS атаки TCP SYN наведено на рис. 2.

```
root@kali:~# hping3 --flood -S -p 80 10.37.129.3
HPING 10.37.129.3 (eth0 10.37.129.3): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Рис. 2. Запуску DDoS атаки TCP SYN на цільову комп'ютерну систему з IP адресою 10.37.129.3

Як видно з першої половини рис. 4, середній час реакції ping в нормальних умовах становить 0,6 мс. Відразу після ініціювання атаки час реакції ping збільшився в середньому до 300 мс. Потрібно відзначити, що в цьому експерименті в атаках використовується лише одна машина. В реальних умовах атаки, яка проводиться із залученням багатьох зомбі-комп'ютерів, число яких може досягати тисяч комп'ютерних систем, наслідки атаки були б значно руйнівнішими. Значення ping, на протязі всього часу проведення DDoS атаки наведено на рис. 3.

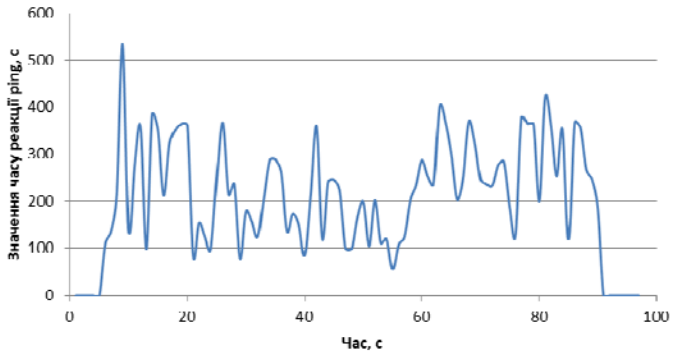

Рис. 3 Значення ping, на протязі проведення DDoS атаки

Рис. 4 Скріншот реакції ping до початку DDoS атаки TCP SYN та після (стрибкоподібне збільшення часу реакції)

Для проведення експерименту DDoS атака тривала приблизно 1,5 хвилини для кожного з протоколів. В результаті було захоплено близько 600 000 пакеті.

Отримання легітимного трафіку

Для збору легітимного трафіку було використано два пристрої IoT, які регулярно взаємодіяли протягом приблизно 12 хвилин. Перший пристрій – датчики руху Fibaro1, які вимірює температуру, освітленість, рух та акселерометр. Датчик підключається через контролер Z-Wave до комп'ютера та інтегрується з OpenHab2. Трафік цього пристрою збирався в автономному режимі на локальному хості. Другий IoT датчик – це модуль камери Raspberry Pi Camera Module V2, що був підключений до Raspberry Pi, та використовувався для передачі потокового відео та розпізнавання обличчя. Камера зафіксувала нерозпізнані обличчя та надіслала зображення в службу простого зберігання (AWS-S3) Amazon Web Service, а також виконувала прямі трансляції. Камера передала з високою якістю HD на машину на базі Ubuntu, а тривалість захоплення трафіку становила близько 4 хвилин.

Таким чином в результаті проведення збору зразків трафіку було отримано навчальну вибірку розміром 24 000 записів, з яких 14 234 були промарковані як DDoS трафік, а 9766 відповідали легітимному трафіку.

Оцінка ефективності виявлення DDoS атак на IoT мережі

З метою визначення ефективності виявлення DDoS атак на IoT мережі було проведено множину експериментів з використанням методу DDoS атак на основі методу логістичної регресії. З цією метою запропонований метод був реалізований у вигляді програмного забезпечення.

Для обчислення показників ефективності було використано 10-fold перехресну перевірку. З цією метою 90% всієї множини тестових даних було використано для навчання моделі і 10% для тестування. Така процедура вибору даних проводилась десять разів, кожного разу вибираючи іншу послідовність для навчання та тестування. Такий алгоритм вибору даних дозволяє змоделювати ситуацію виявлення zero-day шкідливого програмного забезпечення. Загальна ефективність роботи методу визначалась як середнє значення показників ефективності на кожному з десяти етапів тестування. Після кожного етапу тестування було обраховано значення accuracy, precision, recall та F1:

Ефективність виявлення:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{13}$$

Точність виявлення:

$$precision = \frac{TP}{TP + FP}, \tag{14}$$

Повнота виявлення:

$$recall = \frac{TP}{TP + FN}, \tag{15}$$

F1 міра:

$$F1 = 2 \cdot \frac{precision \cdot recall}{precision + recall}, \tag{16}$$

де TP – кількість вірно виявлених вірусних програм, FN – кількість хибно класифікованих вірусних програм, TN – кількість вірно ідентифікованих корисних програм, FP – кількість корисних програм неправильно класифікованих як вірусні програми.

Результати експериментальних досліджень наведені у таблиці 1. За результатами проведеного дослідження найвища ефективність виявлення була досягнута на рівні 91%. Проте при найвищому значені ефективності виявлення рівень помилки першого роду також був найвищий та складав 10%. Після проведення 10 експериментів було визначено середні значення статистичних показників, зокрема значення accuracy становило 89,9%, а рівень хибних спрацювань складав 9,6%. Результати accuracy та помилок першого роду під час проведення 10 експериментів наведено на рис. 5.

Таблиця 1

Результати експериментальних досліджень

№	Спостереження				Метрики			
	TP	FP	TN	FN	Precision	Recall	F1	Accuracy
1	12910	1324	8679	1087	0,9070	0,9223	0,9146	0,8995
2	12936	1298	8777	989	0,9088	0,9290	0,9188	0,9047
3	12809	1425	8664	1102	0,8999	0,9208	0,9102	0,8947
4	13076	1158	8887	879	0,9186	0,9370	0,9277	0,9151
5	12847	1387	8746	1020	0,9026	0,9264	0,9143	0,8997
6	12660	1574	8670	1096	0,8894	0,9203	0,9046	0,8888
7	12766	1468	8867	899	0,8969	0,9342	0,9152	0,9014
8	12782	1452	8803	963	0,8980	0,9299	0,9137	0,8994
9	12866	1368	8561	1205	0,9039	0,9144	0,9091	0,8928
10	12936	1298	8442	1324	0,9088	0,9072	0,9080	0,8908
Сер.	**12859**	**1375**	**8710**	**1056**	**0,9034**	**0,9242**	**0,9136**	**0,8987**

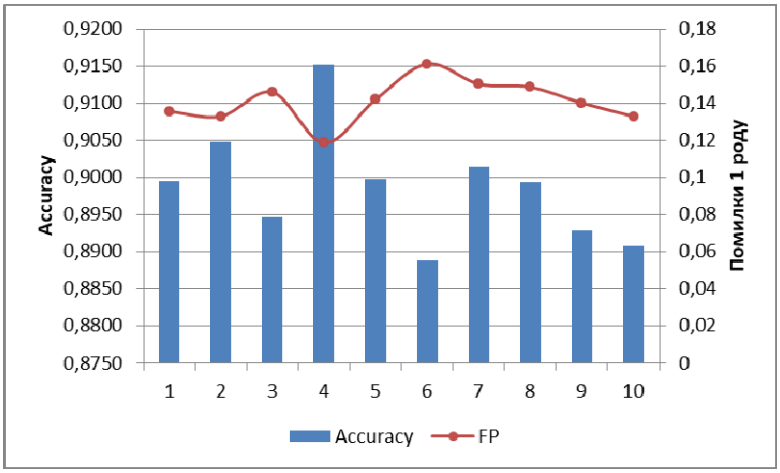

Рис. 5 Значення accuracy та помилок першого роду при проведенні 10 кратної перехресної перевірки

Висновок

Розроблено метод виявлення DDoS атак у IoT-мережах, що заснований на використанні логістичної регресії. В умовах обмежених обчислювальних потужностях та обсягах доступної пам'яті у мережах IoT, використання методу логістичної регресії продиктоване невисокою обчислювальною складністю та простотою його реалізації. Запропонований метод складається з двох етапів: offline та online. Головною метою offline етапу є створення моделі класифікатора, яка буде в подальшому використана в процесі виконання online етапу. Особливістю offline етапу є те, що в процесі навчання моделі логістичного класифікатора весь набір навчальних даних розбивається на два набори. Перший набір даних є маркованим, і він буде використовуватися для тренування класифікатора на основі логістичної регресії. Другий набір даних також є маркованим і використовується для валідації. Алгоритм навчання не використовує мітки набору даних валідації, натомість мітки використовуються для перевірки передбачуваного виходу класифікатора.

Шляхом моніторингу мережевого трафіку в режимі реального часу етап online здійснює виявлення DDoS атак на основі використання сформованої на етапі offline моделі класифікатора. Процес виявлення передбачає розбиття спостережуваного періоду моніторингу на 10 відрізків та визначення на кожному з них проміжних результатів. Висновок про наявність DDoS атаки здійснюється на основі порівняння середнього значення серед всіх проміжних результатів класифікації з пороговим значенням виявлення. У випадку перевищення порогового значення робиться висновок про наявність DDoS атаки.

За результатами проведеного дослідження із застосування розробленого програмного забезпечення найвища ефективність виявлення DDoS атак типу TCP SYN була досягнута на рівні 91%. Проте при

найвищому значені ефективності виявлення рівень помилки першого роду також був найвищий та складав 10%. Після проведення 10 експериментів було визначено середні значення статистичних показників, зокрема значення accuracy становило 89,9%, а рівень хибних спрацювань складав 9,6%.

References

1. Arbor NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report. 23 January 2018. [Online]. URL: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_ Infrastructure_Security_ Report.pdf.

2. Elzen I. v. d. Techniques for detecting compromised IoT Devices / I. v. d. Elzen, J. v. Heugten // MSc System and network Engineering, University of Asterdam. – 2017. – pp. 1-26.

3. Zhang C. Communication security in internet of thing: preventive measure and avoid ddos attack over iot network / C. Zhang, R. Green // Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International. – Alexandria Virginia, 2015. – pp. 8–15.

4. Nobakht M. A host-based intrusion detection and mitigation framework for smart home iot using openflow / M. Nobakht, V. Sivaraman, and R. Boreli // Proceedings of the 11th International Conference in Availability, Reliability and Security (ARES). – Salzburg, Austria, 2016. – pp. 147–156.

5. Jerkins J. A. Motivating a market or regulatory solution to iot in security with the mirai botnet code / J. A. Jerkins // Proceedings of the 7th Annual Computing and Communication Workshop and Conference (CCWC). – Las Vegas, NV, USA, 2017. – pp. 1–5.

6. Jun C. Design of complex event-processing idsin internet of things / C. Jun, C. Chi // Proceedings of the Sixth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). – Zhangjiajie, China, 2014. – pp. 226-229.

7. Xiang Y. Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics / Y. Xiang, K. Li, W. Zhou. // IEEE Transactions on Information Forensics and Security. – 2011– Vol. 6. – No. 2. – pp. 426–437.

8. Du P. IP packet size entropy-based scheme for detection of DoS/DDoS attacks. / P. Du, S. Abe. // IEICE transactions on information and systems. – 2008. – Vol. 91. – Issue 5. – pp. 1274–1281

9. Meidan Y. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders / Y. Meidan, M. Bohadana, Y. Mathov et al. // IEEE Pervasive Computing. – 2018. – Vol. 17. – Issue 3. – pp. 12–22.

Рецензія/Peer review : 13.1.2020 р. Надрукована/Printed :16.2.2020 р.
Стаття рецензована редакційною колегією