УДК 004.056

О.М. Савчук
С.М. Захарченко

ВИКОРИСТАННЯ БАЄСІВСЬКОГО КЛАСИФІКАТОРА ДЛЯ ІДЕНТИФІКАЦІЇ DDOS АТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація
Представлено використання баєсівського класифікатора для захистку комп'ютерних мереж за допомогою ідентифікації та визначення DDOS атак.
Ключові слова: DDoS атаки, комп'ютерні мережі, баєсівський класифікатор, захист комп'ютерних мереж.

Abstract
The use of a Bayesian classifier for the protection of computer networks by identifying and determining DDOS attacks is presented..
Keywords: DDoS attacks, computer networks, Bayesian classifier, protection of computer networks.

Вступ

Сьогодні помітна тенденція до збільшення кількості та посилення атак на комп'ютерні мережі. Потужність окремих атак на відмову в обслуговуванні може сягати 100 Гбіт на секунду[1]. При великій кількості досліджень по темі ідентифікації та захисту комп'ютерних мереж від DDoS атака, дослідження та модифікація засобів боротьби залишаються актуальними. Для мінімізації наслідків від DDoS атак, важливим фактором є виявлення та ідентифікація загроз [2].

Принцип роботи баєсівського класифікатора

Відповідно до «наївної» баєсівського алгоритму, ймовірність приналежності запиту класу визначається за формулою [3]:

$$P(D|C) = \prod_{i=1} P(w_i|C),$$

де w_i- це атрибути заголовку HTTP-запиту, а саме:
— IP адреса, з якої здійснюється вхід на сайт (IP);
— сторінка, яка запитується з даної IP-адреси (url);
— сторінка входу на сайт (referer);
— тип браузера (user_agent);
— тип операційної системи (os);
— країна, з якої йде запит (country);
— метод запиту (method).

Класифікація запитів відбувається за двома класами – DDoS-боти (C) і легітимні користувачі ($\overline{C}$), тому відповідно до формули Байєса утворюються два вирази [4]:

$$P(C|D) = \frac{P(C)}{P(D)} \prod_{i=1}^{n} P(w_i|C)$$

$$P(\bar{C}|D) = \frac{P(\bar{C})}{P(D)} \prod_{i=1}^{n} P(w_i|\bar{C})$$

Розділивши один вираз на інший, в результаті буде:

$$\frac{P(C|D)}{P(\bar{C}|D)} = \frac{P(C)\prod_{i=1}^{n} P(w_i|C)}{P(\bar{C})\prod_{i=1}^{n} P(w_i|\bar{C})}$$

Взявши логарифм всіх цих ступенів, виходить такий вираз:

$$\ln\frac{P(C|D)}{P(\bar{C}|D)} = \ln\frac{P(C)}{P(\bar{C})} + \sum_{\text{ш}} \ln\frac{P(w_i|C)}{P(w_i|\bar{C})}$$

В результаті, запит може бути класифікований наступним чином: це DDoS-бот, якщо $\ln\frac{P(C|D)}{P(\bar{C}|D)} > 0$, в іншому випадку це легітимний користувач.

Висновки

Запропоновано здійснювати класифікацію трафіку по основних показниках з використанням критерію Баєса, що дозволило підвищити ефективність фільтрації хибних запитів, зберігаючи при цьому високий рівень доступності системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Виявлення та ідентифікація DDoS-атак — Режим доступа: http://conf.vntu.edu.ua/allvntu/2015/initki/txt/fesenko.pdf (дата звернення: 10.03.2023)
2. Захист від DDoS-атак — Режим доступа: https://iitd.com.ua/zashchita-ot-ddos-atak/ (дата звернення: 10.03.2023)
3. Christopher D. Manning, Prabhakar Raghavan and Hinrich Schütze, Introduction to Information Retrieval, Cambridge University Press. 2008
4. Наївний метод Байєса — Режим доступа: http://om.univ.kiev.ua/users_upload/15/upload/file/pr_lecture_04.pdf (дата звернення: 10.03.2023)

Савчук Олексій Миколайович – студент групи КІ-21мз, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: alexey250283@gmail.com.

Захарченко Сергій Михайлович – к.т.н., професор кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця.

Savchuk Oleksii – student group CE-21mz, Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: alexey250283@gmail.com.

Zakharchenko Serhii– candidate tech sciences., professor of the Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia.