УДК 004.054:681.324

О. В. Салієва

Д. С. Соколовський

Аналіз та протидія DDoS-атакам за допомогою штучного інтелекту

Вінницький національний технічний університет

Анотація. *Дана робота присвячена аналізу використання штучного інтелекту як ефективного інструменту для протидії DDoS-атакам. Досліджено різноманітні методи використання штучного інтелекту для захисту комп'ютерних мереж від DDoS-атак. Здійснено порівняльну характеристику розглянутих методів.*

Ключові слова: DDoS-атака, штучний інтелект, аналіз трафіку, захист, машинне навчання, автоматизоване реагування, адаптація захисних механізмів, продуктивність мережі.

Abstract*. This paper investigates the use of artificial intelligence as an effective tool to combat DDoS attacks. Various methods of using artificial intelligence to protect computer networks from DDoS attacks are explored. A comparative analysis of the considered methods is carried out.*

Keywords: DDoS attack, artificial intelligence, traffic analysis, protection, machine learning, automated response, defense adaptation, network performance.

Вступ

DDoS-атака (Distributed Denial-of-Service) – це серйозна загроза для сучасних комп'ютерних мереж. Їх мета полягає в перевантаженні цільового сервера або мережі трафіком, роблячи їх недоступними для легальних користувачів. Традиційні методи захисту від DDoS-атак, такі як фільтрація трафіку, перенаправлення трафіку та аутентифікація користувачів, мають ряд обмежень. Їх налаштування може бути складним, вони не завжди адаптуються до нових та складних DDoS-атак, а також можуть негативно впливати на продуктивність мережі.

Штучний інтелект (ШІ) може стати ефективним інструментом для подолання цих обмежень. ШІ може допомогти автоматизувати процес виявлення та блокування DDoS-атак, адаптувати захисні механізми до нових та складних атак, а також мінімізувати вплив на продуктивність мережі.

Результати дослідження

Штучний інтелект може бути використаний для різних аспектів захисту комп'ютерних мереж від DDoS-атак, а саме: аналізу трафіку, автоматичного реагування, адаптації захисних механізмів, мінімізації впливу на продуктивність мережі.

Аналіз трафіку. ШІ дозволяє проводити глибокий аналіз мережевого трафіку та виявляти аномальні патерни, які можуть вказувати на DDoS-атаку. Використання алгоритмів машинного навчання дозволяє автоматично виявляти атаки, навіть якщо вони маскуються під звичайний трафік. K −means clustering – це алгоритм машинного навчання, який використовується для групування даних за схожістю. У контексті аналізу трафіку K −means може бути використаний для групування пакетів за схожими характеристиками, такими як IP-адреса джерела, порт призначення, тип протоколу [1].

Автоматичне реагування. ШІ може бути налаштований на автоматичне реагування на виявлення DDoS-атак. Це може включати блокування шкідливого трафіку, зміну конфігурацій мережевих пристроїв для відхилення атак, а також сповіщення адміністраторів про інцидент. Брандмауер на основі ШІ може аналізувати пакети даних, щоб визначити, чи є вони легітимними чи шкідливими, а також виявляти аномалії в трафіку, які можуть свідчити про DDoS-атаку і автоматично блокувати трафік, який вважається шкідливим [2].

Адаптація захисних механізмів. Однією з ключових переваг використання ШІ є його здатність до адаптації під нові та еволюціонуючі види атак. Завдяки постійному навчанню на основі нових даних, система може швидко адаптувати свої захисні механізми для ефективного протистояння новим загрозам. Як приклад, алгоритми машинного навчання здатні динамічно адаптуватись для визначення аномальних пакетів, що дозволяє краще реагувати на нові типи атак, котрі можуть мати інші характеристики, відмінні від раніше відомих [3].

Мінімізація впливу на продуктивність мережі: ШІ може допомагати зменшити негативний вплив захисних заходів на продуктивність мережі. Шляхом розумного розподілу ресурсів та виявлення шкідливого трафіку перед тим, як він досягне цільових серверів, можна забезпечити оптимальну роботу мережі навіть під час атак [3].

Безліч сервісів сьогодення використовують комбінацію різних методів, включаючи аналіз трафіку, машинне навчання та автоматизовану реакцію на загрози [4].

Прогностична аналітика. ШІ може використовуватися для прогнозування майбутніх DDoS-атак на основі аналізу даних та трендів. Це дозволяє заздалегідь підготувати мережу до можливих загроз та вжити відповідних заходів для забезпечення її безпеки. На сьогоднішній день ряд компаній використовує нейронні мережі задля аналізу та прогнозування потенційних атак та адаптації до них. Очікується, що ШІ буде відігравати все більш важливу роль у захисті від DDoS-атак. Розробляються нові та інноваційні методи використання ШІ для протидії DDoS-атакам. Впровадження ШІ-систем для захисту від DDoS-атак стає все більш поширеним явищем. Ці системи пропонують кращий захист, гнучкість та адаптивність, що робить їх важливим інструментом для забезпечення безпеки комп'ютерних мереж [5].

Таким чином, аналізуючи вищезазначені методи, можна визначити їхні переваги. Так, аналіз трафіку за допомогою штучного інтелекту, зокрема алгоритмів машинного навчання, має вагому перевагу у виявленні атак, які можуть маскуватися під звичайний трафік. Прогностична аналітика відіграє важливу роль у попередженні майбутніх атак, адже на основі даних, трендів та сучасних загроз можна розробляти ефективні стратегії захисту. Автоматичне реагування дозволяє миттєво реагувати на виявлені атаки, зменшуючи час реакції та швидко виконуючи необхідні заходи. Адаптація захисних механізмів дозволяє системі пристосовуватися до нових видів атак, що дозволяє підтримувати високий рівень захисту у постійно змінному середовищі загроз.

Важливим аспектом успішного захисту буде поєднання декількох систем. Наприклад, аналіз трафіку та автоматичне виявлення може стати потужним інструментом для захисту комп'ютерних мереж від DDoS-атак. Система може виявити незвично великий обсяг запитів із певних IP-адрес, що може бути ознакою атаки. Після виявлення таких аномалій система автоматично блокуватиме доступ з цих IP-адрес, перешкоджаючи надмірному навантаженню на сервери та запобігаючи негативним наслідкам для мережі.

Отже, комбінація різних методів захисту, включаючи аналіз трафіку, прогностичну аналітику, автоматичне реагування та адаптацію захисних механізмів, є найбільш ефективним підходом до захисту мереж від DDoS-атак. Такий підхід дозволяє максимально знизити ризики та забезпечити стійкість мережі у випадку атак.

Висновки

Результати досліджень підтверджують, що штучний інтелект може бути дієвим інструментом для захисту комп'ютерних мереж від DDoS-атак. Використання ШІ дозволяє автоматизувати процес виявлення та блокування атак, а також адаптувати захисні механізми до нових та складних загроз. Таким чином, використання штучного інтелекту є перспективним напрямком для захисту комп'ютерних мереж від DDoS-атак, і подальше дослідження та розробка в цій області може сприяти покращенню безпеки і стійкості інформаційних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Scikit-learn: KMeans - Офіційна документація для алгоритму KMeans у Scikit-learn. URL:https://scikitlear-n.org/stable/modules/generated/sklearn.cluster.KMeans.html
2. B. Senthilnayaki, K. Venkatalakshmi, A. Kannan, Intrusion detection using optimal genetic feature selection and SVM based classifier, in: 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 2015, pp. 1–4.
3. Antoni Jaszcz, Dawid Połap, AIMM: Artificial Intelligence Merged Methods for flood DDoS attacks detection Faculty of Applied Mathematics, Silesian University of Technology, Kaszubska 23, 44-100 Gliwice, Poland, Volume 34, Issue 10, Part A, November 2022, pp. 8090-8101.
4. link11 - Artificial Intelligence (AI) for DDoS Mitigation URL: https://www.link11.com/en/glossar/artificial-intelligence-ai-for-ddos-mitigation/https://www.link11.com/en/glossar/artificial-intelligence-ai-for-ddos-mitigation/

5. Bohdan Bebeshkoa, Karyna Khorolskaa, Nataliia Kotenkoa, Oleksander Kharchenkoa, and Tetyana Zhyrova, Use of Neural Networks for Predicting Cyberattacks, Kyiv National University of Trade and Economics, 19 Kioto str., Kyiv, 02000, Ukraine, pp. 213 – 233

Салієва Ольга Володимирівна − доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Соколовський Дмитро Сергійович – студент групи УБ-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: Dmytro.Sokolovskyi@vntu.net

Saliieva Olha V. − Doctor of Philosophy (PhD) in 125 "Cybersecurity", Senior Lecturer, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@vntu.edu.ua

Sokolovskyi Dmytro S. – student of the UB-21b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: Dmytro.Sokolovskyi@vntu.net