УДК 004.89
Б. М. Липа
(Тернопільський національний технічний університет ім. І.Пулюя)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ DDOS АТАК В КОРПОРАТИВНИХ МЕРЕЖАХ

B. M. Lypa

USING ARTIFICIAL INTELLIGENCE FOR DETECTING DDOS ATTACKS IN CORPORATE NETWORKS

DDoS-атаки є серйозним викликом для безпеки мереж та інформаційних систем. Ці атаки спрямовані на перевантаження мережевих ресурсів, збільшення часу відповіді сервера та призводять до відмови в обслуговуванні. У світі, де важлива кожна секунда доступу до інформації, ефективне виявлення та протидія DDoS-атакам стає невід'ємною частиною стратегії безпеки.

Штучний інтелект в контексті виявлення DDoS-атак використовує різні методи машинного навчання, включаючи нейронні мережі та алгоритми глибокого навчання. Ці системи аналізують та вивчають поведінку мережі, виявляючи аномалії та незвичайні патерни, які можуть свідчити про потенційні DDoS-атаки.

Різноманітні алгоритми машинного навчання можуть бути використані для виявлення атак типу "розподілене відмовлення в обслуговуванні" (DDoS), включаючи навчання з учителем, без учителя та навчання з підкріпленням. Алгоритми навчання з учителем тренуються на маркованих даних, де вхідні дані позначені як звичайний або атакуючий трафік. Алгоритм вчиться розпізнавати шаблони, пов'язані з кожною міткою, і може класифікувати новий трафік як звичайний чи атаку. З іншого боку, алгоритми навчання без учителя не вимагають маркування даних. Замість цього вони навчаються розпізнавати шаблони, групуючи дані в групи за схожістю. Аномалії, які не вписуються в жодну з груп, можуть бути індикатором атаки.

Алгоритми навчання з підкріпленням навчаються від свого оточення через зворотний зв'язок у формі винагороди або покарання. У контексті виявлення атак DDoS, алгоритм навчання з підсиленням може отримувати винагороду за правильне виявлення атаки та покарання за помилковий позитивний сигнал. Алгоритми машинного навчання дозволяють виявляти атаки DDoS в реальному часі, забезпечуючи швидке відновлення після атаки. Їх масштабованість дозволяє аналізувати великий обсяг мережевого трафіку, допомагаючи виявляти атаки DDoS у великих мережах. Крім того, алгоритми машинного навчання можуть розпізнавати нові атаки DDoS, адаптуючись до змінних шаблонів мережевого трафіку. Використання технік машинного навчання для виявлення атак типу DDoS пропонує численні переваги.

Алгоритми глибокого навчання, такі як згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN), моделі із довгою короткочасною пам’яттю (LSTM), виявляються високоефективними для виявлення атак DDoS. Вони можуть автоматично аналізувати та розпізнавати складні патерни та аномалії у великому обсязі мережевого трафіку. Генеративно-змагальні мережі (GAN) використовуються для порівняння синтетичних та реальних даних для виявлення аномалій. Ці алгоритми можуть працювати окремо чи в поєднанні, надаючи високу точність у виявленні DDoS-атак у реальному часі.

Використання систем, що базуються на штучному інтелекті, дозволяє ефективно реагувати на DDoS-атаки практично в реальному часі, запобігаючи їм або пом'якшуючи їхні наслідки. Штучний інтелект може адаптуватися до нових даних, що дозволяє системі ефективно реагувати на зміни у методах DDoS-атак. Завдяки високому рівню автоматизації у сфері виявлення, уникаються людські помилки, а забезпечується більш точний аналіз.

Незважаючи на переваги, існують виклики, такі як адаптація до нових видів атак та висока чутливість до помилкових сигналів. Для подолання цих викликів важливо поєднувати ШІ з іншими методами безпеки та регулярно піддавати систему оновленням.

Література.

1. Rudro, Rifat & Sohan, Md & Chaity, Syma Kamal & Reya, Rubina. (2023). Enhancing DDoS Attack Detection Using Machine Learning: A Framework with Feature Selection and Comparative Analysis of Algorithms. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 14. 1185-1192.

2. K. Wehbi, L. Hong, T. Al-salah and A. A. Bhutta, "A Survey on Machine Learning Based Detection on DDoS Attacks for IoT Systems," 2019 SoutheastCon, Huntsville, AL, USA, 2019, pp. 1-6

3. R. Pandey, M. Pandey and A. Nazarov, "Enhanced DDoS Detection using Machine Learning," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-4