УДК 004.8:004.056

ВИЯВЛЕННЯ ГІБРИДНИХ АТАК КОРИСТУВАЧІВ НА РЕЙТИНГИ РЕКОМЕНДАЦІЙНИХ СИСТЕМ

Іщенко А. І.
Науковий керівник – проф. Чалий С. Ф.
Харківський національний університет радіоелектроніки, каф. ШІ
м. Харків, Україна
тел.: +38(050) 593-31-25, e-mail: anton.ishchenko@nure.ua

In today's digital age, shilling attacks have become a growing concern in online communities. Shilling attacks involve the use of fake accounts or paid individuals to artificially promote a product or service, mislead consumers, and manipulate online discussions. As these attacks can undermine trust in online platforms and harm users, there is a pressing need to develop effective methods for detecting and preventing shilling attacks. This study aims to leverage machine learning techniques to detect and mitigate the impact of shilling attacks in online communities.

The objective of my research is to develop and implement effective methods for detecting user attacks on ratings and recommendations within recommendation systems, using machine learning models.

Рекомендаційні системи формують пропозиції товарів та послуг з урахуванням відомих вподобань користувачів. Знання щодо цих вподобань формуються на основі даних щодо попереднього вибору цих споживачів [1]. Такий вибір представляється покупками товарів та послуг, а також їх рейтинговими оцінками. Штучне спотворення рейтингових оцінок змінює пропозиції рекомендаційної системи і вони не будуть відповідати вподобанням конкретного споживача. Таке викривлення відбувається шляхом шилінг-атак. Шилінг-атаки, або атаки фальшивих користувачів на рейтинги, полягають у штучному пониженні рейтингів конкуруючих товарів та послуг і підвищенні рейтингів предметів, які цікавлять атакуючих [2].

Методи виявлення шилінг-атак є важливим напрямком дослідження в галузі рекомендаційних систем. Ці методи дозволяють автоматично визначати та розрізняти між собою повідомлення, які спрямовані на підвищення/зниження рейтингу заданого товару або послуги. Такі методи можуть виявляти паттерни у поведінці користувачів, які можуть свідчити про зловживання, та розрізняти штучні та оригінальні рейтинги. Впровадження методів виявлення шилінг-атак дає можливість підвищити ефективність рекомендацій, а також зменшити кількість помилкових пропозицій в рамкха недобросовісної конкуренції.

Атаки користувачів на рейтинги товарів та послуг можна класифікувати за такими критеріями:

– за масштабами: цілеспрямовані або масові (здійснюються індивідуально або колективно);

– за метою: підвищення або зниження рейтингу, оцінки, або завдання шкоди конкурентам;

– за формою нападу: написання позитивних або негативних відгуків, коментарів або рейтингів.

На практиці шилінг-атаки можуть об'єднуватись, що значно ускладнює виявлення сфальшованих рейтингів. Для вирішення цієї проблеми доцільно сформувати штучну гібридну атаку і перевірити працездатність рекомендаційної системи. Гібридна атака охоплює такі атаки, як стекінг, віральний маркетинг, рейтинг-інфляція та рейтинг-дефляція. Вибір підмножини використаних атак залежить від специфіки конкретного продукту або послуги, на який націлена атака.

Штучна гібридна шилінг-атака є особливо ефективною для перевірки захисту рекомендаційної системи: її важче виявити, оскільки вона може бути націлена як на збільшення, так і на зменшення рейтингу продукту.

Метод виявлення шилінг-атак на основі штучно сформованої гібридної атаки включає наступні етапи:

Етап 1. Вибір кількох різних методів шилінг-атак для атаки на конкретний продукт або послугу.

Етап 2. Створення декількох облікових записів, які будуть використовуватися для штучного збільшення або зниження рейтингу.

Етап 3. Використання обраних методів шилінг-атак для штучного збільшення або зниження рейтингу продукту.

Етап 4. Аналіз результатів атаки та вибір найефективніших методів.

Етап 5. Повторення атаки з використанням найефективніших методів.

Етап 6. Доповнення рекомендаційного алгоритму кроками виявлення атак, які були виявлені на етапі 5 методу.

Метод може бути доповнений періодичною зміною простих методів атак та облікових записів для виявлення нових вразливостей в рекомендаційній системі.

Таким чином, гібридна шилінг-атака є одним з найбільш складних та тонких видів шилінг-атак, який потребує використання кількох методів та облікових записів. Використання штучних гібридних атак дає можливість виявити та усунути вразливості рекомендаційного алгоритму.

Список використаних джерел:

1. Sundar A. P., Li F., Zou X., Gao T., Russomanno E. D., Understanding Shilling Attacks and Their Detection Traits: A Comprehensive Survey. IEEE Access, 8, 171703-171715, 2020, doi: https://doi.org/10.1109/ACCESS.2020.3022962.

2. Gao, M., Yuan, Q., Ling, B., Xiong, Q. (2014). Detection of Abnormal Item Based on Time Intervals for Recommender Systems. The Scientific World Journal, 2014, 1–8. doi: https://doi.org/10.1155/2014/845897.