УДК 004.056.53:004.85

БАГАТОАГЕНТНЕ НАВЧАННЯ З ПІДКРІПЛЕННЯМ ДЛЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Днепров В.А., Зінченко Д.Р..
vladyslav.dneprov@nure.ua, dmytro.zinchenko1@nure.ua
Науковий керівник – доц., к.т.н., Мартовицький В.О.
Харківський національний університет радіоелектроніки, каф. ЕОМ
м. Харків, Україна

This paper explores the application of multi-agent reinforcement learning (MARL) for intrusion detection in modern network environments. The increasing complexity and distributed nature of information systems require adaptive and intelligent security solutions capable of detecting both known and unknown cyber threats. The proposed approach utilizes multiple cooperative agents that analyze network traffic and system behavior in parallel, learning optimal detection strategies through interaction with the environment. Special attention is given to coordination mechanisms between agents and the use of deep reinforcement learning methods to improve detection accuracy. The advantages of MARL-based systems, including scalability, adaptability, and robustness, are discussed alongside challenges such as training instability, computational complexity, and data requirements. The study demonstrates that multi-agent reinforcement learning can significantly enhance the effectiveness of intrusion detection systems in dynamic and large-scale network infrastructures.

Сучасні інформаційні системи характеризуються високим рівнем складності, розподіленістю інфраструктури та постійним зростанням кількості кіберзагроз. Традиційні системи виявлення вторгнень (IDS), що базуються на сигнатурному або статистичному аналізі, часто не здатні ефективно реагувати на нові та складні атаки. У зв’язку з цим актуальним є використання методів штучного інтелекту, зокрема багатоагентного навчання з підкріпленням (Multi-Agent Reinforcement Learning, MARL), яке дозволяє моделювати поведінку розподілених агентів і адаптуватися до змінного середовища в режимі реального часу [1].

Метою роботи є дослідження застосування багатоагентного навчання з підкріпленням для побудови інтелектуальної системи виявлення вторгнень. У такій системі кожен агент відповідає за аналіз певної частини мережевого середовища або окремого типу трафіку. Агенти взаємодіють між собою, обмінюються інформацією та спільно формують рішення щодо наявності аномалій або атак. Такий підхід дозволяє підвищити масштабованість системи та забезпечити більш точне виявлення складних багатовекторних загроз [2].

Основою запропонованої системи є алгоритми навчання з підкріпленням, у яких агенти навчаються на основі взаємодії із середовищем, отримуючи винагороду за правильне виявлення атак та штрафи за помилки. У багатоагентному середовищі важливою є координація дій агентів, що досягається за допомогою механізмів спільного або частково спільного навчання. Сучасні дослідження демонструють ефективність використання MARL для задач кібербезпеки, зокрема для виявлення складних і прихованих атак у мережевому трафіку [3].

Для аналізу мережевого трафіку використовуються як класичні ознаки (швидкість передачі даних, кількість пакетів, типи протоколів), так і високорівневі представлення, сформовані за допомогою глибинних нейронних мереж. Поєднання глибинного навчання та навчання з підкріпленням дозволяє створювати адаптивні моделі, здатні виявляти як відомі, так і нові типи атак. У сучасних роботах також активно застосовуються підходи на основі глибокого Q-навчання та акторно-критичних методів, які забезпечують більш стабільне навчання в умовах складних середовищ [4].

Важливим аспектом є проблема масштабованості та ефективності системи. У розподілених мережах із великою кількістю вузлів централізовані підходи можуть бути неефективними через затримки та обмеження пропускної здатності. Використання багатоагентної архітектури дозволяє розподілити обчислення між агентами та зменшити навантаження на центральні вузли. Крім того, такі системи є більш стійкими до відмов, оскільки вихід з ладу окремих агентів не призводить до повної втрати функціональності [5].

Разом із перевагами, підхід MARL має низку викликів. До них належать складність навчання у багатовимірному середовищі, проблема нестабільності через взаємний вплив агентів, а також необхідність великої кількості навчальних даних. Крім того, важливо забезпечити інтерпретованість рішень системи, що є критичним для застосувань у сфері кібербезпеки.

Отже, багатоагентне навчання з підкріпленням є перспективним підходом до побудови сучасних систем виявлення вторгнень. Воно дозволяє створювати адаптивні, масштабовані та стійкі до змін середовища системи, здатні ефективно виявляти складні кіберзагрози. Подальші дослідження спрямовані на підвищення стабільності навчання, зменшення обчислювальних витрат та інтеграцію таких систем у реальні мережеві інфраструктури.

Список використаних джерел:

1. Nguyen T. T., Reddi V. J. Deep Reinforcement Learning for Cyber Security // IEEE Transactions on Neural Networks and Learning Systems. 2022. DOI: 10.1109/TNNLS.2021.3121873

2. Alavizadeh H., Jang-Jaccard J., Jo E. Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection // Computers & Security. 2022. DOI: 10.1016/j.cose.2021.102675

3. Zolanvari M., Teixeira M. A., Jain R. Machine Learning-Based Network Intrusion Detection: A Survey // IEEE Communications Surveys & Tutorials. 2021. DOI: 10.1109/COMST.2021.3052862

4. Yang, Y., Luo, R., Li, M., Zhou, M., Zhang, W., & Wang, J. (2018, July). Mean field multi-agent reinforcement learning. In International conference on machine learning (pp. 5571-5580). PMLR.

5. Al-Haija Q. A., Al-Badawi A. Multi-Agent Reinforcement Learning for Intrusion Detection Systems // IEEE Access. 2023.