DOI: 10.37791/2687-0649-2026-21-2-102-118 EDN: CMQRNK
Научная статья
ВАК 2.3.6 ГРНТИ 28.23.37, 50.37.23 УДК 004.056.53:004.8

Метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей

И.В. Котенко[1*]***, И.Б. Саенко***[1]***, В.А. Липатников***[2]***, И.А. Андреев***[2]
[1]*Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия*
[2]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Санкт-Петербург, Россия*
[*]*ivkote@comsec.spb.ru*

Аннотация. Рассматривается проблема динамического обнаружения киберугроз в распределенных системах Интернета вещей в условиях ограниченной адаптивности статических систем обнаружения вторжений и уязвимости моделей машинного обучения к состязательным воздействиям. Целью работы является повышение эффективности обнаружения киберугроз в распределенных IoT-системах по критериям результативности и оперативности за счет применения генеративных моделей, способных моделировать нормальное и аномальное поведение узлов с учетом изменчивости среды. Используется метод, основанный на применении генеративно-состязательных моделей и контрастивного обучения для формирования оценки аномальности временных окон IoT-данных и принятия решения по пороговому правилу. Выполнен вычислительный эксперимент на открытом наборе данных N-BaIoT для сценариев атак семейства Mirai, в рамках которого проведена сравнительная оценка статистических, линейных и автоэнкодерных методов обнаружения аномалий на оконном представлении IoT-данных. Показано, что выбранное признаковое описание обеспечивает высокую результативность обнаружения киберугроз при малом времени вывода, а применение автоэнкодера демонстрирует наилучшие значения F1-меры на рассмотренных сценариях. Полученные результаты подтверждают перспективность дальнейшей реализации предложенного генеративного метода для анализа временных последовательностей IoT-трафика и его применения в интеллектуальных средствах мониторинга сетевой безопасности на уровне периферийных узлов и шлюзов IoT-систем.

Ключевые слова: генеративные модели, обнаружение вторжений, аномалии, Интернет вещей, распределенные системы, временные ряды, киберустойчивость, информационная безопасность

Для цитирования: *Котенко И.В., Саенко И.Б., Липатников В.А., Андреев И.А.* Метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей // Прикладная информатика. 2026. Т. 21. № 2. С. 102–118. DOI: 10.37791/2687-0649-2026-21-2-102-118.

DOI: 10.37791/2687-0649-2026-21-2-102-118
Research article

A method for dynamic detection of cyber threats in distributed Internet of Things systems based on generative models

***I. Kotenko*[1*], *I. Saenko*[1], *V. Lipatnikov*[2], *I. Andreev*[2]**
[1]*Saint Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia*
[2]*Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg, Russia*
[*]*ivkote@comsec.spb.ru*

Abstract. The article examines the problem of dynamic cyberthreat detection in distributed Internet of Things systems, addressing the limited adaptability of static intrusion detection systems and the vulnerability of machine learning models to adversarial influences. The aim of the work is to improve the effectiveness of cyberthreat detection in distributed IoT systems based on efficiency and timeliness criteria by using generative models capable of simulating normal and abnormal node behavior while accounting for environmental variability. A method based on generative adversarial models and contrastive learning is employed to generate anomaly estimates for IoT data time windows and make decisions based on a threshold rule. A computational experiment was conducted on the open N-BaIoT dataset for Mirai family attack scenarios, comparing statistical, linear, and autoencoder-based anomaly detection methods on windowed representations of IoT data. It was demonstrated that the selected feature description ensures high cyberthreat detection efficiency with short inference times, and the use of an autoencoder yields the best F1-score values across the scenarios considered. The obtained results confirm the potential for further implementation of the proposed generative method for analyzing IoT traffic time sequences and its application in intelligent network security monitoring tools at the edge and gateway levels of IoT systems.

Keywords: generative models, intrusion detection, anomalies, Internet of Things, distributed systems, time series, cyber resilience, information security

For citation: Kotenko, I., Saenko, I., Lipatnikov, V., & Andreev, I. (2026). A method for dynamic detection of cyber threats in distributed Internet of Things systems based on generative models. *Journal of Applied Informatics, 21*(2), 102–118. https://doi.org/10.37791/2687-0649-2026-21-2-102-118

Введение

Интенсивное развитие технологий Интернета вещей (Internet of Things, IoT) и их внедрение в критически важные и промышленные системы приводит к формированию распределенных сетевых сред с высокой динамикой состояний узлов и сетевого трафика. Увеличение количества взаимодействующих устройств, их гетерогенность и автономность функционирования существенно расширяют поверхность атак и повышают вероятность реализации сложных киберугроз [1, 2]. В таких ус-