УДК 004.832.2

Кузнецова Е.В., Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ V2X-СИСТЕМ

Аннотация. В статье рассматриваются методы машинного обучения (МО), применяемые для обнаружения вторжений в системах V2X (Vehicle-to-Everything). Показана эффективность ключевых алгоритмов МО в контексте обеспечения информационной безопасности автомобильных сетей: метода K-ближайших соседей, многослойного перцептрона, сетей с долгой краткосрочной памятью (LSTM) и деревьев решений. Особое внимание уделено сравнительному анализу их производительности на основе стандартных оценочных метрик.

Ключевые слова: машинное обучение, обнаружение вторжений, V2X, подключенные автомобили, кибербезопасность.

Введение

С развитием технологий V2X, обеспечивающих обмен данными между транспортными средствами и инфраструктурой, резко возросла уязвимость таких систем к киберугрозам [1]. Традиционные методы защиты зачастую не справляются с новыми типами атак, что делает машинное обучение (МО) перспективным инструментом для мониторинга и предотвращения вторжений. В данной работе мы проанализируем современные ML-алгоритмы, доказавшие свою эффективность обеспечения информационной безопасности автомобильных сетей.

Обзор методов машинного обучения

Машинное обучение (ML) представляет собой набор подходов в области искусственного интеллекта, позволяющих разрабатывать компьютерные системы, способные к самообучению [2]. Методы машинного обучения подразделяются на классическое обучение, нейросети и глубокое обучение, обучение с подкреплением, ансамблевое обучение. Как видно из рис. 1, существует большое разнообразие алгоритмов МО.

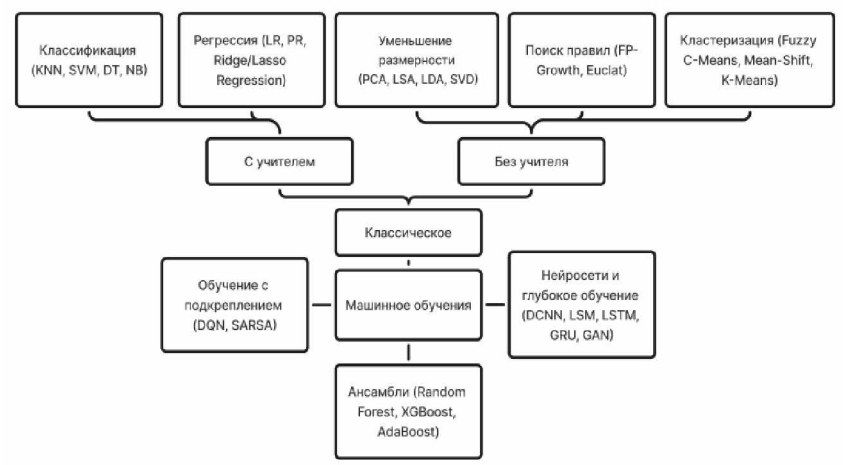

Рис. 1. Алгоритмы машинного обучения

Для систем обнаружения вторжений в V2X чаще всего используются такие модели обучения как: многослойный перцептрон [3], сети с долгой краткосрочной памятью (LSTM), классические методы обучения с учителем [4], среди которых выделяются: метод k-ближайших соседей и деревья принятия решений.

Метод k-ближайших соседей (k-Nearest Neighbor)

Алгоритм KNN, основан на принципе «похожие объекты ведут себя аналогично», и он успешно применяется для классификации устройств в сетях VANET (Vehicular ad-hoc network) [5]. Его ключевое преимущество – простота интерпретации результатов: автомобиль идентифицируется как «доверенный» или «подозрительный» на основе анализа поведения ближайших соседей.

Многослойный перцептрон (MLP, Multi-Layer Perceptron).

MLP – это тип искусственной нейронной сети, который состоит из нескольких слоев нейронов, включая входной слой, один или несколько скрытых слоев и выходной слой. Исследование [6] подтвердило, что такая модель эффективно выявляет отклонения в поведении узлов VANET за счет обучения с обратным распространением ошибки.

Сети с долгой краткосрочной памятью (LSTM, Long Short Term Memory)

Для борьбы с Sybil-атаками в Системах Кооперативного Интеллектуального Транспорта (C-ITS) предложено использовать LSTM [7] – особый тип нейросетей, специализирующийся на анализе временных последовательностей. Хотя метод уступает другим в точности (Таблица 1), его сила в прогнозировании сложных многоэтапных атак.

Деревья решений (DT, Decision Trees)

Деревья решений представляют собой модель, которая принимает решения на основе последовательности вопросов, задаваемых о входных данных. Данный метод основывается на правиле: «Если <условие>, то <ожидаемый результат>». В работе [8] показано, что деревья решений в

CAN-сетях особенно эффективны против атак типа «отказ в обслуживании» и спуфинга.

Сравнительный анализ

Таблица 1 наглядно демонстрирует, что: KNN лидирует по F1-мере (99.37),

MLP достигает рекордного показателя качества (99.40 %), а LSTM имеет сбалансированные, но менее выдающиеся показатели.

Таблица 1

Производительность моделей обучения

Метод	Точность	Полнота	F1-мера	Качество
KNN [9]	98,95	96,23	99,37	97,99
MLP [7]	97,95	97	97,46	99,40
DT [8]	98,19	98,16	-	98,19
LSTM [6]	95,6	89,6	92,5	96,4

Вывод

Проведенное исследование подтверждает, что классические ML-алгоритмы (KNN, DT) и многослойный перцептрон демонстрируют наилучшие результаты в задачах обнаружения вторжений для V2X. Несмотря на потенциал LSTM, применение этого метода неэффективно из-за низких показателей, в особенности показателя полноты. Перспективы для дальнейшей работы – изучение и проектирование гибридных моделей, сочетающих преимущества всех рассмотренных подходов.

Список использованных источников:

1. Lu R., L. Zhang, J. Ni, and Fang Y. “5g vehicleto-everything services: Gearing up for security and privacy,” Proceedings of the IEEE, 2019.

2. IBM machine learning definition. URL: https://www.ibm.com/cloud/learn/machine-learning.

3. Hossain M.D., Inoue H., Ochiai H., Fall D., and Kadobayashi Y., “An effective in-vehicle can bus intrusion detection system using cnn deep learning approach,” in GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.

4. Uprety A., Rawat D.B., and Li J., “Privacy preserving misbehavior detection in iov using federated machine learning,” in 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021.

5. Montenegro J., Iza C., and Aguilar Igartua M., “Detection of position falsification attacks in vanets applying trust model and machine learning,” in Proceedings of the 17th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, 2020.

6. Ghaleb F.A., Zainal A., Rassam M.A., and Mohammed F., "An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications," in 2017 IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2017.

7. Khan I.A., Moustafa N., Pi D., Haider W., Li B., and Jolfaei A., "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles", 2021.

8. Moulahi T., Zidi, S., Alabdulatif A., Atiquzzaman M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. IEEE, 2021.

9. Refat R.U.D.; Elkhail A.A.; Hafeez A.; Malik H. Detecting CAN Bus Intrusion by Applying Machine Learning Method to Graph Based Features. In Intelligent Systems and Applications, Germany, 2022.

Kuznetsova E.V., Sentsova A.U.
Ufa University of Science and Technology, Ufa

APPLICATION OF MACHINE LEARNING IN INSURANCE DETECTION SYSTEMS FOR V2X SYSTEMS

Abstract. The article discusses machine learning (ML) methods used for intrusion detection in V2X (Vehicle-to-Everything) systems. The effectiveness of key ML algorithms in the context of ensuring information security of vehicular networks is demonstrated: K-nearest neighbors method, multilayer perceptron, long short-term memory (LSTM) networks, and decision trees. Particular attention is paid to a comparative analysis of their performance based on standard evaluation metrics.

Keywords: machine learning, intrusion detection, V2X, connected cars, cybersecurity.