УДК 004.89

ГИБРИДНЫЕ МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В ТРАФИКЕ СЕТЕВЫХ ДАННЫХ

Орлова Е.Р., студент гр. 23.М02-мкн, I курс
Санкт-Петербургский политехнический университет Петра Великого,
г. Санкт-Петербург

Гибридные методы машинного обучения для обнаружения аномалий в трафике сетевых данных представляют собой комбинацию различных подходов и алгоритмов, направленных на более точное и эффективное выявление аномалий в сетевом трафике. Такие методы часто сочетают в себе преимущества различных подходов, таких как статистические методы, методы глубокого обучения и традиционные алгоритмы машинного обучения. Давайте рассмотрим некоторые из ключевых принципов и примеры гибридных методов для обнаружения аномалий в сетевом трафике: [1-4]

1. Использование комбинации алгоритмов.

Гибридные методы могут объединять в себе несколько алгоритмов, таких как метод опорных векторов (SVM), случайный лес (Random Forest) и нейронные сети, для создания более надежной и мощной системы обнаружения аномалий.

2. Объединение различных типов признаков.

Гибридные методы могут использовать разнообразные типы признаков, такие как статистические характеристики трафика, временные шаблоны и структурные особенности сетевых данных, для создания комплексного и информативного описания сетевого трафика [5-8].

3. Адаптивное обучение.

Гибридные методы могут использовать механизмы адаптивного обучения, которые позволяют системе обновляться и адаптироваться к изменяющимся условиям и характеристикам сетевого трафика в реальном времени.

4. Использование ансамблей моделей.

Гибридные методы могут использовать ансамбли моделей, объединяя прогнозы от нескольких базовых моделей, что позволяет улучшить качество и надежность обнаружения аномалий.

Примеры гибридных методов для обнаружения аномалий в сетевом трафике включают в себя комбинации методов классификации, кластеризации и алгоритмов глубокого обучения. Например, гибридные методы могут использовать сочетание алгоритма SVM с нейронными сетями для обнаружения

аномалий в сетевом трафике, где SVM используется для идентификации аномалий на основе статистических признаков, а нейронные сети – для анализа сложных шаблонов и зависимостей в данных.

В целом, гибридные методы машинного обучения для обнаружения аномалий в трафике сетевых данных представляют собой эффективный подход к обеспечению безопасности сетей, который объединяет в себе преимущества различных подходов и алгоритмов.

Их применение может помочь выявлять аномалии в сетевом трафике с высокой точностью и надежностью, что является критически важным для обеспечения безопасности информационных систем и защиты от кибератак.

Список литературы:

1. García-Teodoro P. Anomaly-based network intrusion detection: Techniques, systems and challenges / P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez // Computers & Security. – 2009. – Vol. 28, № 1–2. – P. 18–28. – DOI: 10.1016/j.cose.2008.08.003.
2. Buczak A. L. A survey of data mining and machine learning methods for cyber security intrusion detection / A. L. Buczak, E. Guven // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, № 2. – P. 1153–1176. – DOI: 10.1109/COMST.2015.2494502.
3. Aburomman A. A. A novel SVM-kNN-PSO ensemble method for intrusion detection system / A. A. Aburomman, M. B. I. Reaz // Applied Soft Computing. – 2016. – Vol. 38. – P. 360–372. – DOI: 10.1016/j.asoc.2015.10.011.
4. Yin C. A deep learning approach for intrusion detection using recurrent neural networks / C. Yin, Y. Zhu, J. Fei, X. He // IEEE Access. – 2017. – Vol. 5. – P. 21954–21961. – DOI: 10.1109/ACCESS.2017.2762418.
5. Tavallaee M. A detailed analysis of the KDD CUP 99 data set / M. Tavallaee, E. Bagheri, W. Lu, A. A. Ghorbani // Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. – Ottawa : IEEE, 2009. – P. 1–6. – DOI: 10.1109/CISDA.2009.5356528.
6. Moustafa N. UNSW-NB15: a comprehensive data set for network intrusion detection systems / N. Moustafa, J. Slay // Proceedings of the 2015 Military Communications and Information Systems Conference. – Canberra : IEEE, 2015. – P. 1–6. – DOI: 10.1109/MilCIS.2015.7348942.
7. Sharafaldin I. Toward generating a new intrusion detection dataset and intrusion traffic characterization / I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani // Proceedings of the 4th International Conference on Information Systems Security and Privacy. – Funchal : SciTePress, 2018. – P. 108–116. – DOI: 10.5220/0006639801080116.

8. Ring M. A survey of network-based intrusion detection data sets / M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho // Computers & Security. – 2019. – Vol. 86. – P. 147–167. – DOI: 10.1016/j.cose.2019.06.005.