DOI 10.37882/2223-2966.2024.03.24

АНАЛИЗ ПРИМЕНЕНИЯ АДАПТИВНЫХ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ К ЗАДАЧЕ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНУЮ СЕТЬ

ANALYSIS OF THE USE OF ADAPTIVE MACHINE LEARNING METHODS TO THE TASK OF INTRUSION DETECTION IN A COMPUTER NETWORK

S. Nesterov

Summary. *Objective*: to study adaptive machine learning methods used to detect intrusions into computer networks in order to increase the efficiency and accuracy of the threat detection system.
Methods: to achieve this goal, methods of analysis and generalization of the results of scientific research devoted to the development of adaptive algorithms for detecting anomalies in network traffic were used.
Results: as a result of the study, it was shown that the use of adaptive machine learning methods based on incremental learning and the use of artificial neural networks makes it possible to increase the effectiveness of intrusion detection in computer networks. Systems using such methods demonstrate high accuracy and the ability to adapt to changes in the network environment and attack methods. The results of the study confirm the prospects of using adaptive machine learning methods in the field of information security and the need for their further development.

Keywords: analysis, task, adaptive method, network.

Нестеров Сергей Геннадьевич
Аспирант, Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет»
nesterov.s.g@edu.mirea.ru

Аннотация. *Цель*: исследование адаптивных методов машинного обучения, применяемых для обнаружения вторжений в компьютерные сети с целью повышения эффективности и точности системы обнаружения угроз.
Методы: для достижения поставленной цели применялись методы анализа и обобщения результатов научных исследований, посвященных разработке адаптивных алгоритмов выявления аномалий в сетевом трафике.
Результаты: в результате исследования было показано, что применение адаптивных методов машинного обучения, основанных на инкрементном обучении и использовании искусственных нейронных сетей, позволяет повысить эффективность обнаружения вторжений в компьютерные сети. Системы, использующие такие методы, демонстрируют высокую точность и способность адаптироваться к изменениям в сетевой среде и методам атак. Результаты исследования подтверждают перспективность использования адаптивных методов машинного обучения в области информационной безопасности и необходимость их дальнейшего развития.

Ключевые слова: анализ, задача, адаптивный метод, сеть.

Введение

С течением времени подходы к обнаружению вторжений претерпевали существенные изменения, начиная от классических специализированных систем обнаружения вторжений (СОВ), требующих ручного анализа информации системными администраторами, и заканчивая поколением более эффективных автоматических систем. Современные СОВ успешно выявляют достаточно широкий спектр сетевых атак. Тем не менее, постоянное возникновение новых методов и техник их осуществления приводит к тому, что многие атаки могут остаться незамеченными. Существующие СОВ в условиях динамичной сетевой среды либо не способны постоянно охватывать всё новые возникающие модели атак, либо делают это недостаточно оперативно в виду необходимости обновления баз правил вручную. Стремительное развитие информационных технологий, сопровождающимся быстрым изменением параметров среды и стратегий атак, требует, чтобы СОВ, призванные обеспечивать наблюдение за сетевым трафиком в вычислительной сети, обладали способностью адаптироваться к изменениям в сетевой среде, в которой они функционируют.

Несмотря на наличие исследований, посвященных данному вопросу, полученные результаты исследований носят разрозненный характер, необходима их систематизация и обобщение полученных результатов. Отсутствует четкое определение понятия «адаптивная система обнаружения вторжений». В данной статье будут рассмотрены некоторые предлагаемые модели адаптивного обнаружения вторжений с целью формирования представления о достижениях и полученных результатах в этой области, а также выявления недостатков предложенных решений. Это позволит представить современное состояние проблемы и внести вклад в её решение в дальнейших исследованиях.

Развитие подходов к обнаружению вторжений

Система обнаружения вторжений (СОВ) — это программное или аппаратное средство, осуществляющее мониторинг и анализ событий в компьютерных сетях и си-

стемах с целью выявления признаков нарушений политики безопасности и атак на информационные ресурсы [12].

Первые СОВ были узкоспециализированными. Процесс обнаружения вторжений требовал применения знаний и опыта экспертов по информационной безопасности в области анализа данных аудита, определении нормального профиля активности, создания и понимания сигнатур атак. Их функционирование ограничивалось единственной целевой средой, которая в свою очередь не была статической, а изменялась со временем. В результате такие ранние СОВ не могли детектировать новые техники атак. Чтобы соответствовать растущему объёму и сложности в результате развития информационных технологий передаваемого сетевого трафика, было предложено новое поколение СОВ. Исследования и технологии в области обнаружения вторжений перешли к новой концепции — подходам на основе сбора и анализа данных (Data Mining-подходы).

Существует два основных подхода к обнаружению атак — обнаружение аномалий и обнаружение злоупотреблений [11]. Обнаружение аномалий основано на предположении, что системе известны некоторые признаки, характеризующие нормальное или допустимое поведение объекта наблюдения, тем самым СОВ на основе обнаружения аномалий приобретает возможность выявлять некоторые неизвестные виды атак. С другой стороны, метод обнаружения злоупотреблений основывается на том, что СОВ известны некоторые признаки, характеризующие поведение злоумышленника. Чаще всего заранее известные действия атакующего задаются с помощью шаблонов (сигнатур) атак. На текущий момент большинство российский и западных разработок СОВ в качестве основного метода обнаружения вторжений используют именно сигнатурные методы [4], а методы на основе обнаружения аномалий чаще всего применяются в качестве дополнения. Это объясняется надёжностью и высоким уровнем интерпретируемости результатов работы первых, несмотря на возможность обнаружения только явно описанных видов атак. В то же время применение систем на основе технологии обнаружения аномального поведения на практике ограничено такими недостатками, как необходимость длительного и качественного обучения, высокий уровень ложных срабатываний и потребность в большом количестве вычислительных ресурсов [12, с. 35].

Таким образом, рост числа полиморфных вредоносных программ и сложных стратегий атак выявил недостатки и этих систем, что продемонстрировало необходимость в разработке более совершенных адаптивных СОВ.

Адаптивность в СОВ

Адаптивная СОВ — это система обнаружения вторжений, использующая адаптивные алгоритмы и способная автономно развиваться и совершенствовать свои механизмы обнаружения в ответ на постоянно меняющееся поле угроз информационной безопасности. Адаптивность включает в себя несколько аспектов, в том числе гибкость при внедрении новых знаний, гибкость при смене парадигм обнаружения и сохранение эффективности на фоне появления новых векторов атак. Адаптивная СОВ характеризуется способностью обучаться на основе непрерывного потока данных, используя алгоритмы и модели, которые позволяют динамически обновлять базу знаний без прямого участия человека [28].

Чаще всего адаптивные алгоритмы реализуются с помощью методов машинного обучения. В отличие от классических алгоритмов, которые обучают модель на фиксированном наборе данных, адаптивные алгоритмы способны изменять свои параметры и поведение в реальном времени, чтобы учитывать новые данные и изменения в окружающей среде, например, изменение количества узлов, характера сетевого трафика и др. Одним из самых перспективных методов адаптивного машинного обучения является инкрементное обучение искусственных нейронных сетей, при котором новые данные обрабатываются постепенно во время работы, модифицируя уже существующую модель [9]. Другим зарекомендовавшим себя подходом к созданию адаптивных СОВ является применение искусственных иммунных систем.

Обзор литературы

В настоящее время направление развития СОВ в сторону адаптивности модели обнаружения как никогда популярно [2]. Существует множество исследований, предлагающих различные адаптивные алгоритмы выявления аномалий в сетевом трафике, основанные на таких методах машинного обучения как k-ближайших соседей (k-NN) [18, 21, 24, 27], метод опорных векторов (SVM) [19, 20, 29], метод k-средних (K-means) [10], дерево принятия решений (Decision Tree) [27], наивный байесовский классификатор (Naive Bayes) [17, 25] и байесовская сеть [1, 14], нечёткую логику [8], глубокое обучение [5, 6], ансамбли методов [13, 15, 16]. Под адаптивностью в большинстве из них понимается способ повышения эффективности обнаружения угроз с помощью алгоритмов интеллектуального анализа данных, основанный на предварительном обучении системы с целью приобретения способности обнаруживать ранее не встречающиеся угрозы. В основе данного понимания адаптивности лежит обобщающая способность. Однако обобщение также имеет свои ограничения и со временем достигает своего предела из-за новых методов атак, которые значительно отличаются от уже изученных. Предлагаемые в перечисленных исследованиях адаптивные СОВ не предусматривают автономного обучения и обновления в режиме реального времени.

Биоинспирированный метод обнаружения вторжений, основанный на применении искусственных иммунных системах предложен в статье [7]. Авторами был разработан алгоритм отрицательного отбора для обнаружения аномалий. Данный подход позволяет генерировать детекторы, которые участвуют в обнаружении аномалий. Проведенное тестирование метода продемонстрировало, что точность алгоритма составляет в среднем 96 % на наборе данных KDDCup99. В работе [3] также представлена гибридная модель СОВ с использованием искусственных иммунных систем. Производительность СОВ с точки зрения показателя частоты обнаружения (полноты) оказалась не очень высокой — 92,59 %, 75,02 %, 66,87 % и 63,39 % для классов Probe, DOS, U2R и R2L соответственно.

В некоторых других научных работах отдельно уделяется внимание вопросу онлайн-обучения СОВ. Так, в статье [23] предложена модель для обнаружения и предотвращения атак «нулевого дня» с использованием инкрементного обучения LMAD/PZ. В работе были исследованы и реализованы две инкрементные техники интеллектуального анализа данных — квазиоптимальный алгоритм контролируемого машинного обучения (AQ) и неконтролируемый алгоритм кластеризации Cobweb. Проведенное тестирование в онлайн-режиме этих алгоритмов показало, что AQ превосходит Cobweb по многим критериям и демонстрирует точность 93,3 %. Кроме того, бесспорным преимуществом AQ является возможность выражения нормального и аномального сетевого трафика в форме генерируемых атрибутивных правил.

Проблеме создания адаптивной СОВ посвящена статья [26]. Предложенное авторами решение основано на концепции машины экстремального обучения (Extreme Learning Machine) и способно обнаруживать обучаться на шаблонах данных как от существующих, так и новых типах атак. Предлагаемая СОВ способна функционировать как в режиме неконтролируемого обучения, так и контролируемого, получая данные об атаках от эксперта и обновляясь в соответствии с ними, затрачивая при этом сравнительно немного вычислительных ресурсах.

В научной статье [22] предложен фреймворк самообучаемой СОВ (SSID) для IoT-систем, позволяющей обучаться на поступающих пакетах трафика в реальном времени. Предлагаемая модель анализирует и маркирует входящие пакеты трафика, основываясь только на решениях самой СОВ с использованием глубокой автоассоциативной случайной нейронной сети, а также на онлайн-оценке ее статистически измеренной достоверности. Сравнение SSID с другими существующими работами, в которых реализовано самоконтролируемое обучение, показывает её преимущество перед последними. Автономное и инкрементное обучение показывают лучшие результаты чем SSID на небольших объёмах данных, в связи с тем, что SSID не проходит предварительного обучения и не требует готовых наборов данных. Но с увеличением объёма данных для обучения, точность SSID должна превышать существующие аналоги.

Обсуждение

Большинство исследований, предлагающих новые методы обнаружения вторжений, направлены на повышение эффективности работы СОВ, увеличение показателя точности, сокращение времени обучения и т.д. СОВ на основе машинного обучения, и, в частности, ансамблях методов, действительно показывают очень хорошие результаты по сравнению с традиционными сигнатурными подходами.

Однако ни одна модель, основанная на «статичных» традиционных алгоритмах машинного обучения, не способна точно и последовательно обнаружить все виды атак. Одна из причин этого — постепенное изменение характеристик сетевой среды функционирования и постоянная модификация техник атак.

Кроме того, существующие модели СОВ обучаются и тестируются на образцах сетевого трафика из конкретных, чаще всего устаревших наборов данных. Представленные в них примеры скорее всего не будут соответствовать реальной сети, в которой планируется использовать СОВ. В результате точность классификации сетевого трафика на практике будет существенно ниже экспериментальных данных. Кроме того, проведенный в предыдущем исследовании сравнительный анализ различных методов машинного обучения для обнаружения вторжений показал, что для использования готовых наборов необходима их предварительная обработка [2]. Вопросы предобработки данных, удаления незначимых признаков и устранения дисбаланса представленных классов атак до сих пор являются предметом активного изучения.

Применение адаптивных методов машинного обучения в СОВ способно устранить многие недостатки современных подходов. Но, к сожалению, сами они также не лишены недостатков, требующих устранения. Например, при использовании инкрементного или онлайнового обучения наиболее сильно проявляются проблема катастрофического забывания и дилемма стабильности-пластичности. Тщательного исследования требуют и вопросы обеспечения безопасности и стабильности адаптивных моделей, используемых в СОВ, к которым предъявляются особые требования. Уязвимым местом многих СОВ на основе машинного обучения является подверженность состязательным атакам.

Заключение

Современные СОВ, основанные на алгоритмах интеллектуального анализа данных, демонстрируют высокую эффективность в выявлении различных видов угроз. Однако необходимо учитывать ограничения таких моделей, включая необходимость постоянного обновления и адаптации к новым методам атак. Проведенный анализ показал, что в большинстве работ не уделяется должного внимания вопросам динамического развития и обновления модели обнаружения вторжений.

Дальнейшее развитие в области адаптивных методов машинного обучения для обнаружения вторжений требует обращения внимания не только повышению точности и эффективности систем, но и обеспечению их устойчивости к новым видам атак и изменениям в сетевой среде. Важно разрабатывать модели, способные оперативно адаптироваться к динамике угроз и обеспечивать надежную защиту информационных ресурсов.

В целом, адаптивные методы машинного обучения играют ключевую роль в современной кибербезопасности и их дальнейшее развитие и совершенствование являются приоритетными задачами для обеспечения безопасности информационных систем и защиты конфиденциальности данных.

ЛИТЕРАТУРА

1. Арустамов С.А., Дайнеко В.Ю. Применение динамической байесовской сети в системах обнаружения вторжений // Научно-технический вестник информационных технологий, механики и оптики. — 2012. — №3 (79). — С. 128–133.
2. Бурлаков М.Е. Оценка эффективности адаптивных алгоритмов в системе обнаружения вторжений / М.Е. Бурлаков // Инновации в науке и практике: Сборник статей по материалам VII международной научно-практической конференции. В 5-ти частях. — Барнаул, 2018. — Т. 2. — С. 83–92.
3. Бурлаков М.Е. Система обнаружения вторжения на основе искусственной иммунной системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. — 2019. — № 29. — С. 209–224.
4. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А., Никольская А.Г. Применение глубокого обучения для обнаружения компьютерных атак в сетевом трафике // Труды ИСП РАН. — 2023. — Т. 35, вып. 4. — С. 65–92.
5. Зуев В.Н. Обнаружение аномалий сетевого трафика методом глубокого обучения // Программные продукты и системы. — 2021. — №1. — С. 91–97.
6. Иванов А.Д., Кутищев А.А., Никитина Е.Ю. Разработка приложения для анализа сетевого трафика и обнаружения сетевых атак // Вестник Пермского университета. Математика. Механика. Информатика. — 2021. — № 2. — С. 57–64.
7. Коробейников А.Г. Разработка алгоритма для системы обнаружения вторжений на основе искусственных иммунных систем // Международный журнал гуманитарных и естественных наук. — 2021. — № 11-3(62). — С. 21–25.
8. Корышев Н.П. Построение системы обнаружения вторжений на основе нечёткого классификатора и алгоритма «китов» // Сборник избранных статей научной сессии ТУСУР. — 2021. — № 1-2. — С. 196–200.
9. Орлов А.А., Абрамова Е.С. Разработка и исследование алгоритма посменного инкрементного обучения нейронной сети // Компьютерная оптика. — 2023. — Т. 47, № 3 — С. 491–497.
10. Ряполова Е. Разработка алгоритма подсистемы обнаружения вторжений / Е. Ряполова, М. Студянникова // Первая миля. — 2022. — № 3(103). — С. 70–80.
11. Труфанов В.Н., Нестеров С.Г., Огарок А.Л. Исследование сетевых систем обнаружения вторжений, использующих методы машинного обучения // Информатизация и связь. — 2023. — № 4. — С. 59–72.
12. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие для вузов / под ред. О.И. Шелухина. — Москва : Горячая линия-Телеком, 2020. — 220 с.
13. Aburomman A., Reaz M. A novel SVM-kNN-PSO ensemble method for intrusion detection system // Applied Soft Computing. — 2016. — Vol. 38. — pp. 360–372.
14. Cemerlic A., Yang L., Kizza J.M. Network Intrusion Detection Based on Bayesian Networks // In Proceedings of SEKE. — 2008. — P. 791–794.
15. Gao X., Shan C., Hu C., Niu Z., Liu Z. An Adaptive Ensemble Machine Learning Model for Intrusion Detection // IEEE Access. — 2019. — Vol. 7. — pp. 82512–82521.
16. Ge L., Zhang H., Li H. Novel Ensemble Method Based on Improved k-nearest Neighbor and Gaussian Naive Bayes for Intrusion Detection System // Advanced Intelligent Computing Technology and Applications. — 2023. — Vol. 14087. — pp. 737–748.
17. Huang Y. Network Intrusion Detection Method Based on Naive Bayes Algorithm // 6th Asian Conference on Artificial Intelligence Technology (ACAIT), Changzhou, China, 2022, pp. 1–10.
18. Karimi Z., Torabi Z. An Adaptive k-nearest neighbor Classifier using Differential Evolution with Auto-Enhanced Population Diversity for Intrusion Detection // Research Square. — 2022.
19. Khodaskar M., Medhane D., Ingle R., Buchade A. Khodaskar A. Feature-based Intrusion Detection System with Support Vector Machine // IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS). Pune, India. 2022. pp. 1–7.
20. Kim G., Lee S., Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection // Expert Syst. Appl. — 2014. — Vol. 41. — pp. 1690–1700.
21. Liao Y., Vemuri V.R. Use of K-Nearest Neighbor classifier for intrusion detection // Computers & Security. — 2002. — Vol. 21(5). — pp. 439–448.
22. Nakıp M., Gelenbe E. Online Self-Supervised Learning in Machine Learning Intrusion Detection for the Internet of Things, 2023, https://arxiv.org/abs/2306.13030v1.
23. Nasr A.A., Ezz M.M., Abdulmaged M.Z. An Intrusion Detection and Prevention System based on Automatic Learning of Traffic Anomalies // International Journal of Computer Network and Information Security(IJCNIS). — 2016. — Vol.8, No.1. — pp. 53–60.

24. Onyezewe A., Kan, A.F., Abdullahi F.B., Abdulsalami, A.O. An Enhanced Adaptive k-Nearest Neighbor Classifier Using Simulated Annealing // International Journal of Intelligent Systems and Applications. — 2022. — Vol. 13. — pp. 34–44.
25. Panda M., Patra M.R. Network intrusion detection using naïve bayes // IJCSNS International Journal of Computer Science and Network Security. — 2007. — Vol.7, No.12. — pp. 258–263.
26. Roshan S., Miche Y., Akusok A., Lendasse A. Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines // Journal of the Franklin Institute. — 2018. — Vol. 355(4). — pp. 1752–1779.
27. Singh A.P., Kumar S., Kumar A., Usama M. Machine Learning based Intrusion Detection System for Minority Attacks Classification // International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES). Greater Noida, India. 2022. pp. 256–261.
28. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // Proceedings of the IEEE Symposium on Security and Privacy. — 2010.
29. Thaseen I.S., Kumar C.A. Intrusion detection model using fusion of chi-square feature selection and multi class SVM // Journal of King Saud University — Computer and Information Sciences. — 2017. — Vol. 29, Issue 4. — pp. 462–472.