Автоматизация и моделирование в проектировании и управлении. 2022. № 2 (16). С. 13-17.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2022. № 2 (16). P. 13-17.

Научная статья
Статья в открытом доступе
УДК 004
doi:10.30987/2658-6436-2022-2-13-17

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМ УЗЛОМ С ИСПОЛЬЗОВАНИЕМ БЕСПРОЕКТОРНЫХ АЛГОРИТМОВ СТОХАСТИЧЕСКОЙ АППРОКСИМАЦИИ ПРИ НЕСАНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЯХ ВХОДНОГО ПОТОКА

Кирилл Станиславович Ткаченко
Севастопольский государственный университет, г. Севастополь, Россия
KSTkachenko@sevsu.ru

Аннотация. *Цель работы: в настоящей работе предлагается подход принятия решений для управления компьютерным узлом в условиях несанкционированных изменений входного трафика. Методы исследования: в работе используются аналитическое моделирование систем массового обслуживания и алгоритмы стохастической аппроксимации. Результаты исследования и новизна: в работе получен подход на основе алгоритмов стохастической аппроксимации для адаптивного принятия решений при априорной неопределенности входных данных. Выводы: полученный подход позволяет увеличить эффективность функционирования компьютерных систем при несанкционированных вторжениях.*

Ключевые слова: аналитическое моделирование, алгоритмы стохастической аппроксимации, системы массового обслуживания, компьютерные узлы

Для цитирования: Ткаченко К.С. Управление компьютерным узлом с использованием беспроекторных алгоритмов стохастической аппроксимации при несанкционированных изменениях входного потока // Автоматизация и моделирование в проектировании и управлении. 2022. №2 (16). С. 13-17. doi: 10.30987/2658-6436-2022-2-13-17.

Original article
Open Access Article

CONTROLLING A COMPUTER NODE USING PROJECTOR-LESS STOCHASTIC APPROXIMATION ALGORITHMS FOR UNAUTHORIZED INPUT FLOW MODIFICATIONS

Kirill S. Tkachenko
Sevastopol State University, Sevastopol, Russia
KSTkachenko@sevsu.ru

Abstract. *The aim of the work is to propose a decision-making approach for managing a computer node in the face of unauthorized input traffic modifications. The research methods are analytical modelling of queuing systems and stochastic approximation algorithms. The results of the research and novelty are to obtain an approach based on the stochastic approximation algorithms for adaptive decision making under a priori uncertainty of input data. Findings of the obtained approach allow increasing the efficiency of computer systems in case of unauthorized intrusions.*

Keywords: analytical modelling, stochastic approximation algorithms, queuing systems, computer nodes

For citation: Tkachenko K. S. Controlling a computer node using projector-less stochastic approximation algorithms for unauthorized input flow modifications. Automation and modeling in design and management, 2022, no. 1 (15). pp. 15-23. doi: 10.30987/2658-6436-2022-2-13-17.

Введение

В наши дни повседневная практика эксплуатации сложных компьютерных систем показывает, что дальнейшее развитие различных существующих управляющих инфраструктур играет существенную роль при формировании принципиально новых

подходов к развитию управляемых объектов. Разнообразность в имеющихся аппаратно-программных комплексах затрудняет реализацию запланированных их изменений, поскольку могут требоваться определенные уточнения для соответствия всем актуальным условиям и состоянию окружающих сложных систем. Значимость этих уточнений может, в некоторых ситуациях, повлиять на сложившиеся корректировочные процессы, что, в свою очередь, потребует модернизации процессов анализа работы компьютерных систем в условиях имеющихся ресурсных (в том числе, финансовых) ограничений. Поэтому в настоящей работе рассматриваются подходы к управлению компьютерным узлом с использованием беспроекторных алгоритмов стохастической аппроксимации при несанкционированных изменениях входного потока. Системы выбора на основе беспроекторных алгоритмов могут позволить отбросить несущественные варианты выбора и, таким образом, нивелировать неблагоприятные воздействия.

Необходимость в обеспечении поддержки защитных средств

Для обеспечения транспортировки с использованием беспилотных транспортных средств требуется наличие защищенной и безопасной компьютерной инфраструктуры [1]. Безопасная инфраструктура позволит одновременно достичь эффективную транспортировку за счет исключения влияния человеческого фактора. В частности, эффективность повышается при наличии возможности непрерывного мониторинга состояния окружающей среды и внутренних систем и соответствующих изменений в работе транспортных средств, а также планирования необходимых для функционирования средства изменений. В состав компьютерной инфраструктуры средств могут входить разнообразные программно-аппаратные датчики и программно-управляющие комплексы. Эти комплексы, в наиболее общем случае, могут содержать подсистемы искусственного интеллекта. Могут производиться различные реализации угроз компьютерной безопасности, в том числе, и вторжения в системы, эксплуатация уязвимостей, компрометация измеряемых величин и многое другое. В беспилотных транспортных средствах следует однозначно применять меры по управлению компьютерными узлами информационных подсистем, чтобы существовала возможность для компенсации, либо исключения уязвимостей.

Автоматизированные банковские системы также подвержены рискам, связанным с компьютерными вторжениями [2]. Компьютерные вторжения в такие автоматизированные системы влияют на банковские бизнес-процессы. Ликвидация их последствий во многих случаях является невозможной при отсутствии структурных описаний задействованных в банкинге средств. Риски можно оценить количественно, и во многих случаях для вычисления искомой оценки рисков следует использовать подходы на основе методов теории вероятностей. В частности, существуют такие вероятностные модели, которые позволяют выявить уязвимое место электронного банкинга. Известно, что риски приводят к ошибкам и проблемам в функционировании систем электронного банкинга, снижают эффективность протекания их бизнес-процессов. Для оценки рисков, в первую очередь, определяются возможные величины денежных потерь. Степень риска, оцененная по таким потерям, может варьироваться от допустимой до критической.

Для защиты информации всегда необходимы средства для выявления вторжений и других угроз [3]. Эти средства могут быть основаны на различных моделях и методах, позволяющих количественно, с различной степенью точности, оценить значения характеристик компьютерных систем, в том числе, с учетом реализации рисков безопасности. Для построения моделей используются данные, накопленные в журналах событий операционной системы, полученные от сканеров уязвимостей, систем управления событиями безопасности, антивирусов и многих других. С помощью методов систем искусственного интеллекта можно получить соотношения и взаимосвязи отдельных событий безопасности. Следует обязательно учитывать и сложность имеющихся структур и информационных потоков в аппаратурной составляющей, поскольку, в некоторых особен-

ных ситуациях, атаки могут привести к выходу из строя и аппаратных подсистем.

Построение систем компьютерной защиты во многих случаях сопряжено с применением дедуктивных методов для построения деревьев решений [4]. В отличие от индуктивных методов построения, в определенных ситуациях получаемые дедуктивными методами деревья могут быть нечувствительны к шумам, а также требуют меньших объемов выборок для построения. Эти методы сводят возникающие задачи для обеспечения компьютерной защиты к некоторым известным задачам принятия решений, которые могут быть решены различными способами, в том числе, и с использованием деревьев решений. С помощью таких деревьев организуется проверка и разрешение доступа к информационным и прочим ресурсам компьютерных систем с учетом существующей политики информационной безопасности. Для построения таких деревьев важны, в первую очередь, формальные модели, описывающие существующие, возможно, сложные структуры компьютерных систем.

Беспроекционные алгоритмы для обеспечения безопасности

Поэтому можно использовать подходы на основе алгоритмов стохастической аппроксимации для адаптивного принятия решений при априорной неопределенности входных данных [5 – 7]. Эти алгоритмы дополняют существующие подходы по принятию решений на основе результатов аналитического моделирования систем массового обслуживания (СМО) [8 – 10].

Среди алгоритмов стохастической аппроксимации для адаптивного принятия решений при априорной неопределенности входных данных можно отметить алгоритмы Нарендры-Шапиро, Льюса, Варшавского-Воронцовой, Буша-Мостеллера, Назина-Позняка, которые могут быть реализованы как компоненты программного комплекса для поддержки принятия решений [11]. В основе таких алгоритмов лежит использование рандомизированных стратегий на *n* шагах функционирования:

$$p_{n+1} = R_n(x_1, \dots, x_n; p_1, \dots, p_n; \xi_1, \dots, \xi_n), n = 1,2, \dots \quad (1)$$

где R_n – вектор-функция со значениями в симплексе S^N; p_n – вектор условных вероятностей выбора вариантов $x(1), \dots, x(N)$ в момент времени t_n с учетом известных потерь $\xi_1, \dots, \xi_n$ от выбора варианта. Перед выбором очередного варианта x_{n+1} происходит расчет p_{n+1} по (1). Выбор варианта осуществляется методом деления отрезка с учетом элемента случайности ω_n. Такие рандомизированные стратегии могут обеспечить минимум предельных значений средних текущих потерь $\lim_{n\to\infty} \frac{1}{n}\sum_{j=1}^{n} \xi_j$ [5].

Если значение вектор-функции ограничено $R_n \in [0; 1]$, то необходимости в операторе проецирования на симплекс S^N нет. Тогда используются так называемые беспроекторные алгоритмы, в частности, Нарендры-Шапиро, Льюса, Варшавского-Воронцовой, Буша-Мостеллера.

Пусть варианты выбора $x(1), \dots, x(N)$ соответствуют определенным программно-аппаратным конфигурациям с различными емкостями буфера $N_{x(k)}$, числом каналов обслуживания $K_{x(k)}$ и их производительностью $\mu_{x(k)}$ для выбранного варианта $x(k)$, модельно реализованных на основе СМО. Тогда функционирование процессов принятия решений для управления компьютерным узлом с использованием беспроекторных алгоритмов стохастической аппроксимации при несанкционированных изменениях входного потока можно укрупненно описать следующими подшагами для каждого шага *n* длительностью *T*:

n.1. На шаге *n* для измеренной величины функции текущих потерь ξ_n и интенсивности входного потока заявок λ_n по формуле (1) определяется очередное значение вектора условных вероятностей выбора вариантов p_{n+1}.

n.2. С учетом элемента случайности ω_n производится выбор варианта функционирования компьютерной системы $x(k)$, а именно, устанавливаются априори

заданные емкости буфера $N_{x(k)}$, число каналов обслуживания $K_{x(k)}$ и их производительность $\mu_{x(k)}$.

Для шагов n = 1, 2,… подшаги n.1, n.2 могут быть выполнены не только для отдельного выбранного компьютерного узла защищаемой компьютерной инфраструктуры, но и для всех компьютерных узлов этой инфраструктуры параллельно. Применение подхода позволяет минимизировать средние потери, в том числе и от несанкционированных вторжений.

Заключение

На основе алгоритмов стохастической аппроксимации для адаптивного принятия решений при априорной неопределенности входных данных и аналитического моделирования СМО можно построить эффективное управление компьютерными узлами инфраструктуры для минимизации средних текущих потерь от несанкционированных вторжений. Системы выбора на основе беспроекторных алгоритмов могут позволить отбросить несущественные варианты выбора и увеличить эффективность функционирования компьютерных систем.

Список источников:

1. Чучаев А.И., Грачева Ю.В., Маликов С.В. Посягательства на информационную систему беспилотника в этиологии дорожно-транспортных происшествий // Всероссийский криминологический журнал. 2021. т. 15. №1, С. 55-67.
2. Бердюгин А.А., Ревенков П.В. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации) // Финансы: теория и практика, т. 24, №6. 2020. С. 51-60.
3. Маликов А.В., Авраменко В.С., Саенко И.Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы. №6 (103). 2019. С. 32-42.
4. Токарев В.Л. Формальные модели безопасности // Чебышевский сборник, т. 22. №1 (77). 2021. С. 488-495.
5. Назин А.В., Позняк А.С. Адаптивный выбор вариантов: Рекуррентные алгоритмы. М.: Наука, 1986. 288 с.
6. Ткаченко К.С. Программная система для выбора вариантов на основе проекционных и беспроекционных алгоритмов // Системы контроля окружающей среды. 2016. №3(23). С. 59-62.
7. Ткаченко К.С. Поддержка принятия решений в распределенных средах и однородных сетях алгоритмами стохастической аппроксимации // Алгоритмы, методы и системы обработки данных. 2014. №3(28). С. 69-73.
8. Скатков А.В., Ткаченко К.С. Статистические оценки рисков в условиях несанкционированных возмущений узлового трафика // Системы контроля окружающей среды. Севастополь: ИППС. 2016. Вып. 5 (25). С. 41-46.
9. Ткаченко К.С. Совершенствование средств компьютерной безопасности в организациях путем проведения узловой параметрической корректировки // Вестник Прикамского социального института. 2021. № 2 (89). С. 87-92.
10. Ткаченко К.С. Обеспечение гарантоспособного

References:

1. Chuchaev A.I., Gracheva Yu.V., Malikov S.V. Attacks on the Information System of the Drone in the Etiology of Road Traffic Accidents. All-Russian Criminological Journal. 2021. 15(1):55-67.
2. Berdyugin A.A., Revenkov P.V. Cyberattack Risk Assessment in Electronic Banking Technologies (the Case of Software Implementation).Finance: Theory and Practice. 2020;24(6):51-60.
3. Malikov A.V., Avramenko V.S., Saenko I.B. Model and Method for Diagnosing Computer Incidents In Information and Communication Systems Based on Deep Machine Learning. Information and Control Systems. 2019; (103):32-42.
4. Tokarev V.L. Formal Security Models. Chebyshevskii Sbornik. 2021;22(1):488-495.
5. Nazin A.V., Poznyak A.S. Adaptive Choice of Variants: Recursive Algorithms. Moscow: Nauka; 1986.: 288.
6. Tkachenko K.S. Software System for Selecting Options Based on Projection and Non-Projection Algorithms. Monitoring Systems of Environment. 2016;3(23):59-62.
7. Tkachenko K.S. Decision Support in Distributed Environments and Homogeneous Networks by Stochastic Approximation Algorithms. Algorithms, Methods and Data Processing Systems. 2014;3(28): 69-73.
8. Skatkov A.V., Tkachenko K.S. Statistical Risk Assessments in Conditions of Unauthorized Disturbances of Nodal Traffic. Monitoring Systems of Environment. Sevastopol: NTSI. 2016;5(25):41-46.
9. Tkachenko K.S. Improving Computer Security Tools in Organizations by Performing Nodal Parametric Adjustment. Bulletin of Prikamsky Social Institute. 2021;2(89):87-92.
10. Tkachenko K.S. Ensuring the Guaranteed

функционирования системы обработки данных при интервальных изменениях поточных характеристик на основе аналитического моделирования // Автоматизация и моделирование в проектировании и управлении. 2021. №3-4 (13-14). С. 25-30.
11. Ткаченко К.С. Программный комплекс информационного обеспечения принятия решений в распределенных средах // Свидетельство о регистрации программы для ЭВМ 2021617213, 13.05.2021. Заявка № 2021613477 от 16.03.2021.

Functioning of the Data Processing System with Interval Changes in Flow Characteristics Based on Analytical Modelling. Automation and Modelling in Design and Management. 2021;3-4(13-14):25-30.

11. Tkachenko K.S. Software Complex for Information Support of Decision Making in Distributed Environments. The Certificate on Official Registration of the Computer Programme in Russia no. 2021617213; 2021.

Информация об авторах:

Кирилл Станиславович Ткаченко
инженер 1-й кат. кафедры «Информационные технологии и компьютерные системы» ФГАОУ ВО «Севастопольский государственный университет», г. Севастополь, Россия

Information about authors:

Kirill Stanislavovich Tkachenko
first rank engineer of the Department «Information Technologies and Computer Systems» of Federal State Autonomous Educational Institution of Higher Professional Education «Sevastopol State University», Sevastopol, Russia

Статья поступила в редакцию 16.02.2022; одобрена после рецензирования 03.03.2022; принята к публикации 10.03.2022.

The article was submitted 16.02.2022; approved after reviewing 03.03.2022; accepted for publication 10.03.2022.

Рецензент – Аверченков А.В., доктор технических наук, профессор, Брянский государственный технический университет.

Reviewer – Averchenkov A.V., Doctor of Technical Sciences, Professor, Bryansk State Technical University.