

Представлены результаты экспериментов по анализу эффективности информационной технологии критериального обнаружения атак и оценке уровня достоверности А-событий. Получены оценки ошибок первого и второго рода при классификации состояния трафика телекоммуникационной сети. Проведены эксперименты с целью исследования влияния на уровень правдоподобия различных объемов тестирующих выборок; адаптивного изменения значения метрик правил, а также различных значений весовых коэффициентов, которые задавались экспертом; были проведены специальные эксперименты для различных типов атак. Полученные результаты имеют статистически устойчивый характер и в целом презентативно отображают особенности предложенного подхода. Предложенные методы статистического моделирования и оценки вероятностей допущения ошибок первого и второго родов при обнаружении атак позволяют повысить обоснованность принимаемых решений с учетом рисков. Метод параметрической идентификации системных характеристик телекоммуникационной сети, отличается от известных использованием аналитических моделей многоэтапных процессов деградации и восстановления функциональных характеристик объектов сети.

4. Предлагаемая адаптивная модель обнаружения атак и возможных уязвимостей в компьютерных сетях на основе методов интеллектуального анализа данных может являться основой для ИТ-технологий обеспечения компьютерной безопасности в условиях адаптации при быстром изменении состояния сетевого трафика. Использование адаптивной модели системы принятия решений позволяет повысить уровень правдоподобия распознавания событий, минимизировать число ложных тревог, а также обеспечить высокую реактивность системы, что особенно важно для этапов раннего обнаружения.

Перспективы развития работ по теме связаны с широким использованием методов обеспечения компьютерной безопасности в современных информационных, распределенных, облачных технологиях, применяемых в различных областях человеческой деятельности.

Библиографический список использованной литературы

1. Информационные технологии для критических инфраструктур: моногр./ Под ред. А.В.Скаткова — Севастополь. СевНТУ, 2012. — 306с.
2. Kabiri P. Research in Intrusion Detection and Response. — A Survey/ P.Kabiri, A. Ghorbani. — International Journal of Network Security. — №:1, 2005. — P. 84–102.
3. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов — М.: Наука и Техника, 2004г. — 384с.
4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев — М.: ТИД "ДС", 2002 г. — 688с.

Bryukhovetskyi A.A., Skatkov A.V., Voronin D.Y., Lovyagin V.S. Methodology of construction of intrusion detection system for computer networks.

Presents a comprehensive approach to building Intrusion Detection System, which combines two complementary technologies. The first allows you to recognize the threat of network intrusion and is based on data mining techniques, while the second uses the information on changes in the vector system performance computer network.

Key words: detection of network attacks, information security critical systems.

УДК 004.75

К.С. Ткаченко

Севастопольский национальный технический университет

ул. Университетская 33, г. Севастополь, Россия, 299053

e-mail: tkachenkokirillstanislavovich@mail.ru, tkachenkokirillstanislavovich@gmail.com

АЛГОРИТМ ДОМИНИРУЮЩЕГО ВЫБОРА ВАРИАНТОВ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ ВИРУСНОЙ АТАКИ

Предлагается алгоритм стохастической аппроксимации с выбором доминирующего варианта. Приводятся результаты вычислительного эксперимента.

Ключевые слова: стохастическая аппроксимация.

Как известно [1 — 4], необходимыми составляющими любых современных сложных систем являются средства адаптивного выбора вариантов, в том числе и для динамической реконфигурации в условиях вирусной атаки. Перспективными алгоритмами для решения задач адаптивного выбора в условиях априорной неопределенности входных данных являются рекуррентные алгоритмы, предназначенные для решения задач безусловной минимизации [1]. Поэтому задача разработки нового

алгоритма стохастической оптимизации является актуальной и перспективной. Предлагается проекционный алгоритм стохастической аппроксимации с использованием соседних вариантов, который может позволить решать задачи выбора с измененными характеристиками описательных статистик результатов функции средних значений текущих потерь. Поведение стохастических автоматов с формируемой структурой [1 — 2] можно использовать для отыскания минимума функции в условиях априорной неопределенности входных данных. Такой автомат представляет собой алгоритм изменения вероятностей выбора очередного значения аргумента минимизируемой функции. При этом может формироваться последовательность управляющих воздействий для адаптации систем с дискретным управлением с использованием рекуррентных рандомизированных процедур стохастической аппроксимации. Поэтому в общем случае проблема состоит в анализе и синтезе алгоритмов для нахождения стратегии управления, представляющих собой последовательность управляющих воздействий — вариантов из некоторого конечного дискретного множества, причем эта последовательность может обеспечить минимум предельных средних текущих потерь. Важными научными и практическими задачами, где может потребоваться применение данного алгоритма, являются задачи во многих областях науки и техники [1 — 4]. Различные методы и подходы к решению различных задач адаптивного выбора приведены в работах [1 — 4]. В работе [3] предлагается алгоритм оптимизации с бинарной функцией потерь, в работе [4] — стохастический автомат с переменной структурой с собственной рандомизированной стратегией. Нерешенной ранее частью общей проблемы является модификация нескольких компонентов вектора вероятностей выбора для метода деления отрезка вообще, в случае беспроекционных алгоритмов, или же до применения оператора проектирования, как в случае проекционных.

Целью данной работы является приведение алгоритма доминирующего выбора вариантов, а также его реализации в программно-инструментальном средстве информационного обеспечения принятия решений при априорной неопределенности входных данных.

Рандомизированные стратегии [1] используют рекуррентные правила:

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

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 . Перед выбором очередного варианта x_{n+1} происходит расчет p_{n+1} по (1). Выбор варианта осуществляется методом деления отрезка. Необходимо ввести оператор проектирования. Пусть для любого $q \in R^N$ вектор-столбец $p = \pi_{\varepsilon}^N\{q\}$, принадлежащий $(N-1)$ -мерному единичному ε -симплексу

$$S_{\varepsilon}^N = \left\{ p = (p_1, \dots, p_N) \mid p \in R^N, \sum_{i=1}^N p_i = 1, p_i \geq \varepsilon (i = 1, \dots, N) \right\} \quad (2)$$

определяется условием $\|\pi_{\varepsilon}^N\{q\} - q\| = \min_{p \in S_{\varepsilon}^N} \|p - q\|$. Для любого $q \in R^N$ вектор $\pi_{\varepsilon}^N\{q\}$ существует и единственен

и $q = \pi_{\varepsilon}^N\{q\}$ тогда и только тогда, когда $q \in S_{\varepsilon}^N$. Известны эффективные алгоритмы адаптивного выбора вариантов [1], которые можно подразделить на беспроекционные алгоритмы адаптивного выбора вариантов вида $p_{n+1} = p_n - \gamma_n R(x_n, p_n, \xi_n)$ и проекционные алгоритмы адаптивного выбора вариантов вида $p_{n+1} = \pi_{\varepsilon_{n+1}}^N\{p_n - \gamma_n R(x_n, p_n, \xi_n)\}$, где $R(x_n, p_n, \xi_n) = R_n$ — вектор движения алгоритма, $\gamma_n > 0$ — скалярный множитель — длина шага, $n = 1, 2, \dots$ — номер шага, $\varepsilon_n \in [0, N^{-1})$ — параметр проектора $\pi_{\varepsilon_n}^N$ (2) на n -ом шаге. Для удобства описания обозначения выбора конкретного элемента в векторе можно ввести обозначения $e_i^N = \left(\underbrace{0, \dots, 0}_i, \underbrace{1, 0, \dots, 0}_{N-i} \right)$, $e^N = (1, \dots, 1) \in R^N$, $e(x) = \sum_{i=1}^N e_i^N \chi(x = x(i))$, если $X = \{x(1), \dots, x(N)\}$.

Если $\xi_n = \xi_n(x_n, \omega)$ — случайные потери за выбор варианта x_n , произведенный в момент времени t_n , и ω — элементарный исход, то алгоритмы могут обеспечивать безусловную оптимизацию по критерию минимума U предельных значений средних текущих потерь Φ_n :

$$\Phi_n = \frac{1}{n} \sum_{i=1}^n \xi_i, \quad \lim_{n \rightarrow \infty} \Phi_n \rightarrow \nu. \quad (3)$$

Проекционные алгоритмы возможно объективно лучше беспроекционных, поскольку их можно использовать для решения более широкого класса задач с критериями (3) (как с бинарными, так и с небинарными потерями ξ_n за счет обеспечения нормировки использованием оператора проектирования).

Предлагаемый алгоритм функционирует следующим образом. Вначале происходят прогоны с

фиксированным вариантом, номер варианта постоянен и равен номеру прогона. Затем происходит непосредственно функционирование, выбранным номером варианта является вариант, для которого имеется наименьшее значение среднего от средних величин текущих потерь. Если таких вариантов несколько, используется с наименьшим порядковым номером. Для последующего построения рекуррентной последовательности управляющих воздействий используется алгоритм Назина-Позняка [1]:

$$p_{n+1} = \pi_{e_{n+1}}^N \left\{ p_n - \gamma_n \frac{\xi_n - \Delta}{e^T(x_n) p_n} e(x_n) \right\} \quad (4)$$

В (4) Δ — параметр, влияющий на величину «зазора» между средним значением текущих потерь и ее предельным значением. В отличие от оригинального использования этого алгоритма, начальными значениями компонентов вектора вероятностей выбора вариантов становятся $\left(N^{-1}, \dots, N^{-1}, \frac{kN^{-1}}{N_{domv}}, N^{-1}, \dots, N^{-1} \right)$, где N_{domv} — номер доминирующего варианта, $k=5$ — масштабный множитель, выбранный исходя из общесистемных соображений. Перед первым использованием элементы вектора корректируются оператором проектирования для обеспечения условия нормировки (2).

Для исследования работы алгоритма, в силу того, что происходит управление выбором вариантов, разумно использовать тестовую задачу, в которой число вариантов $N=5$, а потери ξ_n при выборе варианта соответствуют значению элемента вектора $(2, 3, 1, 4, 5)$, причем номер варианта соответствует номеру элемента в векторе. Тестовая задача — «заглушка» изображена на рисунке 1, где V_i — вариант № i .

Результаты работы программной системы сведены в таблицу 1, причем №№ с 1 по 5 соответствуют этапам подстройки и выбора доминирующего варианта, а № 6 отображает результаты функционирования алгоритма по Назину-Позняку с выбором доминирующего варианта при первоначальной инициализации вектора условных вероятностей выбора вариантов.

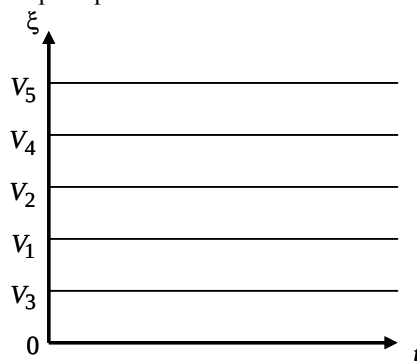


Рисунок 1 — Тестовая задача

Таблица 1 — Результаты (сред. — среднее, std.ош. — стандартная ошибка, std.откл. — стандартное отклонение, дисп. — выборочная дисперсия, диап. — диапазон, мин. — минимум, макс. — максимум)

№	Сред.	Стд.ош.	Стд.откл.	Дисп.	Диап.	Мин.	Макс.
1.	2,000000	0,000000	0,000000	0,000000	0,000000	2,000000	2,000000
2.	3,000000	0,000000	0,000000	0,000000	0,000000	3,000000	3,000000
3.	1,000000	0,000000	0,000000	0,000000	0,000000	1,000000	1,000000
4.	4,000000	0,000000	0,000000	0,000000	0,000000	4,000000	4,000000
5.	5,000000	0,000000	0,000000	0,000000	0,000000	5,000000	5,000000
6.	2,745840	0,018012	0,254730	0,064888	1,975000	1,000000	2,975000

Для проверки предложенных алгоритмов и их программной реализации отладочные сведения о значениях вектора условных вероятностей выбора вариантов сведены в таблицу 2, а в качестве математического ожидания текущих потерь фигурирует величина $\sum_{i=1}^5 V_i p(i)$. В таблице 2 МО тек.потерь — математическое ожидание текущих потерь.

Разработанный алгоритм применен в инструментальном средстве поддержки принятия решений по динамическому реконфигурированию в распределенных средах. Перспективами дальнейших изысканий в данном направлении станут увеличение количества влияющих на функцию текущих потерь параметров

(а именно, планируется добавить к оценке уровень шума и частоту съема данных).

Таблица 2 — Значения элементов вектора вероятностей выбора вариантов на последних шагах (этап подготовки и шаги от 191 до 200)

Шаг	Вариант 1	Вариант 2	Вариант 3	Вариант 4	Вариант 5	МО тек.потерь
Предв.	0,040000	0,040000	0,840000	0,040000	0,040000	1,400000
191	0,061160	0,095645	0,498229	0,138815	0,206151	2,493500
192	0,080606	0,115091	0,517675	0,061032	0,225597	2,396271
193	0,087556	0,122041	0,489872	0,067983	0,232547	2,465777
194	0,094882	0,129368	0,460568	0,075309	0,239874	2,539039
195	0,102655	0,137140	0,429479	0,083081	0,247646	2,616761
196	0,121807	0,060531	0,448631	0,102233	0,266798	2,616761
197	0,173404	0,112129	0,500228	0,153831	0,060408	2,100787
198	0,060286	0,140408	0,528508	0,182110	0,088688	2,242184
199	0,066991	0,147113	0,501689	0,188815	0,095392	2,309232
200	0,074036	0,154158	0,473507	0,195861	0,102438	2,379687

Библиографический список использованной литературы

1. Назин А.В. Адаптивный выбор вариантов: Рекуррентные алгоритмы / А.В. Назин, А.С. Позняк. — М.: Наука, 1986. — 288 с.
2. Назин А.В. О повышении эффективности автоматных алгоритмов адаптивного выбора вариантов / А.В. Назин // Адаптация и обучение в системах управления и принятия решений. — Новосибирск: Наука, 1982. — С. 40—46.
3. Скаткова Н.А. Гарантоспособные технологии реконфигурации автоматизированных транспортно-производственных систем / Н.А. Скаткова // Радіоелектронні і комп'ютерні системи. Вип. 6. — Харьков, 2008. — С. 52—57.
4. Воронин Д.Ю. Обеспечение высокой терминальной готовности на основе информационных технологий распределения ресурсов / Д.Ю. Воронин // Вісник СевНТУ: зб. наук. пр. Вип. 114/2011. Серія: Інформатика, електроніка, зв'язок. — Севастополь, 2011. — С. 100—105.

Tkachenko K.S. Dominant option selection algorithm for action under viral attack.

An algorithm of stochastic approximation with the choice of the dominant variant proposed. The results of computational experiments are given.

Keywords: stochastic approximation.

УДК 004.457

Ю.В. Сосновский, доц., канд. техн. наук

Д.О. Зганяйко

Таврический национальный университет им. В.И. Вернадского

пр. Вернадского 4, г. Симферополь, Россия, 295000

E-mail: mailsender256@mail.ru, zdo.str@gmail.com

А.В. Скатков, проф., д-р техн. наук

Д.Ю. Воронин, канд. техн. наук

Севастопольский национальный технический университет

ул. Университетская 33, г. Севастополь, Россия, 299053

МЕТОДОЛОГИЯ И ВЫБОР ПЕРСПЕКТИВНЫХ НАПРАВЛЕНИЙ РЕАЛИЗАЦИИ СИСТЕМЫ СБОРА ХАРАКТЕРИСТИЧЕСКИХ ДАННЫХ СЕТЕВОГО ТРАФИКА¹⁶

Рассматривается методология построения системы сбора коррелированного набора статистических и сигнатурных данных сетевого трафика. Осуществлен анализ перспективных направлений в реализации указанной системы.

Ключевые слова: сетевой трафик, поддержка принятия решения, сбор характеристических данных

Скрининговый анализ сетевого трафика с целью обнаружения в нем аномальных, деструктивных последовательностей до сих пор является актуальной задачей, несмотря на значительное число аппаратных и программных средств, нацеленных на решение данной проблемы. Причины столь

¹⁶ Работа выполнена при финансовой поддержке РФФИ (грант № 14-41-01564).