Научная статья
УДК 519.61+539.1
https://doi.org/10.31854/1813-324X-2024-10-3-104-115

Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT

Олег Иванович Шелухин, sheluhin@mail.ru
Сергей Юрьевич Рыбаков ✉, svolkov97@gmail.com
Анна Вячеславовна Ванюшина, a.v.vaniushina@mtuci.ru

Московский технический университет связи и информатики,
Москва, 111024, Российская Федерация

Аннотация

Актуальность. *Изменение фрактальной размерности сетевого трафика может служить индикатором атак или аномальной активности. Фрактальный анализ позволяет выявлять изменения временной структуры трафика и сигнализировать о возможных угрозах. Наблюдаемое в широких временных масштабах самоподобие указывает на мультифрактальную природу аномалий, что требует дальнейшего изучения. Таким образом, разработка методов для обнаружения и классификации кибератак с использованием мультифрактального анализа является актуальной задачей для повышения информационной безопасности.*

Цель работы. *Повышение эффективности обнаружения и классификации компьютерных атак в сетях IoT методами машинного обучения за счет расширения количества атрибутов, характеризующих параметры мультифрактального спектра фрактальной размерности.*

Методы исследования: *дискретный вейвлет анализ, мультифрактальный анализ, машинное обучение, программная реализация комбинированного метода многоклассовой классификации в совокупности с методами фрактального анализа.*

Результаты. *Разработана методология оценки характеристик мультифрактального спектра фрактальной размерности трафика с помощью последовательности текущих оценок фрактальной размерности в окне анализа фиксированной длины в зависимости от интервала разрешения (времени дискретизации). Приведены аналитические результаты экспериментальных оценок мультифрактального анализа обрабатываемых процессов в сетях IoT. Оценена информационная значимость дополнительных атрибутов компьютерных атак и нормального трафика для случая бинарной и многоклассовой классификации по индексу Джини для двух случаев: без добавления мультифрактального спектра фрактальной размерности и с добавлением мультифрактального спектра фрактальной размерности. Показано, что основная концентрация наиболее значимых атрибутов приходится на интервал дискретизации 500 мс…1,5 с*

Новизна. *Введено понятие мультифрактального спектра фрактальной размерности в виде последовательности текущих оценок фрактальной размерности в окне анализа фиксированной длины в зависимости от интервала разрешения.*

Практическая значимость. *Представленный метод оценки параметров мультифрактального спектра фрактальной размерности является универсальным и может быть применен в различных информационных системах.*

Ключевые слова: *фрактальная размерность, мультифрактальный анализ, алгоритмы, информационная значимость, компьютерные атаки, статистические характеристики, метрики*

Ссылка для цитирования: Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 104–115. DOI:10.31854/1813-324X-2024-10-3-104-115. EDN:KIRCNK

Original research
https://doi.org/10.31854/1813-324X-2024-10-3-104-115

Estimation of the Multifractal Spectrum Characteristics of Fractal Dimension of Network Traffic and Computer Attacks in IoT

Oleg I. Sheluhin, sheluhin@mail.ru
Sergey Y. Rybakov ✉, svolkov97@gmail.com
Anna V. Vanyushina, a.v.vaniushina@mtuci.ru

Moscow Technical University of Communications and Informatics,
Moscow, 111024, Russian Federation

Annotation

Relevance. Changes in the fractal dimension of network traffic can serve as an indicator of attacks or anomalous activity. Fractal analysis allows to identify changes in the temporal structure of traffic and signal possible threats. The self-similarity observed over wide time scales indicates the multifractal nature of the anomalies, which requires further study. Thus, the development of methods for detecting and classifying cyber attacks using multifractal analysis is an urgent task to improve information security.

The aim of the article. Increasing the efficiency of detection and classification of computer attacks in IoT networks using machine learning methods by expanding the number of attributes characterizing the parameters of the multifractal spectrum of fractal dimension.

Research methods: discrete wavelet analysis, multifractal analysis, machine learning, software implementation of a combined multiclass classification method in conjunction with fractal analysis methods.

Results. A methodology has been developed for assessing the characteristics of the multifractal spectrum of the fractal dimension of traffic using a sequence of current estimates of the fractal dimension in an analysis window of a fixed length depending on the resolution interval (sampling time). The analytical results of experimental assessments of multifractal analysis of processed processes in IoT networks are presented. The informational significance of additional attributes of computer attacks and normal traffic is assessed for the case of binary and multi-class classification using the Gini index for two cases: without adding a multifractal spectrum of fractal dimension and with the addition of a multifractal spectrum of fractal dimension. It has been shown that the main concentration of the most significant attributes falls on the sampling interval of 500 ms...1.5 s.

Novelty. The concept of a multifractal spectrum of fractal dimension is introduced in the form of a sequence of current estimates of the fractal dimension in an analysis window of a fixed length depending on the resolution interval.

Practical significance. The presented method for estimating the parameters of a multifractal spectrum of fractal dimension is universal and can be applied in various information systems.

Keywords: *fractal dimension, multifractal analysis, algorithms, information significance, computer attacks, statistical characteristics, metrics*

For citation: Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Estimation of the Multifractal Spectrum Characteristics of Fractal Dimension of Network Traffic and Computer Attacks in IoT. *Proceedings of Telecommunication Universities.* 2024;10(3):104–115. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-104-115. EDN:KIRCNK

Постановка задачи

Многочисленные исследования статистических характеристик сетевого трафика, сетевых аномалий и компьютерных атак (КА) показывают наличие у них свойств фрактальности или самоподобия, а также изменчивость показателей, характеризующих фрактальные свойства [1–3]. Для их оценки используются понятия фрактальной размерности (ФР) множества D по Хаусдорфу и пока-

затель Херста *H*, характеризующий степень самоподобия процесса, связанные между собой соотношением*: D* = 2 – *H.* В подавляющем большинстве работ в области телекоммуникаций [2–4] используется именно показатель Херста *H, отличающийся от D на фиксированную величину*. Поэтому в дальнейшем в качестве оценки ФР нормального трафика и КА будем использовать именно его.

Методы фрактального анализа широко используются для обнаружения атак и сетевых аномалий, в том числе в режиме реального времени путем мониторинга текущей ФР трафика компьютерных сетей [4]. Формализуя различие спектров трафика с аномалиями и без них, можно сравнивать фрактальные и корреляционные размерности, а также интервалы, характеризующие «ширину» спектра Лежандра для каждой из реализаций.

Информационные размерности сравниваемых реализаций различаются на небольшую постоянную величину и практически не зависят от количества уровней разложения. Это позволяет сделать вывод о том, что наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, и данное свойство можно использовать для выявления атак. Учитывая, что для оценки ФР трафика требуется, как правило, значительные интервалы времени и большие объемы данных, обнаружение КА с помощью фрактального анализа осуществлялось, как правило, независимо от других методов, позволяющих определить аномалии во временно́м ряду в режиме реального времени. Все это послужило поводом для поиска новых методов обнаружения и прогнозирования, к числу которых можно отнести комбинацию машинного обучения и фрактального анализа. Появились работы, в которых вопросы обнаружения и классификации КА стали интегрироваться с методами машинного обучения [4–7].

В работе [5] на примере базы данных KDD Cup1999 [7, 8] показано положительное влияние оценки самоподобных свойств сетевого трафика, характеризуемого средним значением показателя Херста на качество бинарной классификации. Авторы установили, что добавление в число атрибутов дополнительного параметра, характеризующего ФР атак, положительно влияет на эффективность бинарной классификации и справедливо для всех алгоритмов, представленных в исследовании.

В работах [5, 6] на примере набора данных UNSW-NB15 приведены результаты исследования влияния широкого спектра статистических характеристик ФР на качество бинарной классификации. Показано, что параметры ФР могут рассматриваться как дополнительные информационные признаки (атрибуты) КА. В качестве дополнительных признаков предложено использовать широкий спектр статистических характеристик ФР, обрабатываемых последовательностей. Эффективность предлагаемого метода оценивается путем оценки качества бинарной классификации сетевых атак и нормального трафика. С помощью алгоритмов машинного обучения показано, что использование в качестве дополнительных информационных признаков статистических характеристик ФР позволяет повысить ее эффективность в среднем на 10 %.

В работах [8, 9] проанализирован алгоритм обнаружения КА на компьютерные сети, базирующийся на оценке самоподобия аномалий в сетевом трафике с использованием статистических методов. Алгоритм состоит из трех этапов, в рамках которых выполняется анализ свойства самоподобия для эталонного трафика, фрактальных свойств реального трафика и дополнительной обработки временны́х рядов статистическими методами на заключительном этапе. Программная реализации предложенного подхода подтвердила высокую эффективность проанализированного алгоритма.

В [10] предложено использовать для обнаружения аномальных выбросов в системах передачи данных метод машинного обучения, основанный на применении гибридной искусственной нейронной сети, состоящей из автокодировщика (autoencoder) и классификатора. Экспериментальная оценка предлагаемой методики подтвердила ее достаточно высокую эффективность.

В [11] представлен метод выявления аномалий сетевого трафика, основанный на утверждении о том, что последний является самоподобной структурой и моделируется фрактальным броуновским движением. В качестве инструментов при разработке метода были применены фрактальный анализ и математическая статистика. Проведен анализ существующих методов выявления сетевых аномалий на предмет их недостатков. Результатом работы является модифицированный метод выявления аномалий сетевого трафика. Данный метод относится к полуконтролируемой методике обнаружения аномалий, что позволяет процессу быть практически автономным от человеческого вмешательства. Алгоритм поиска аномалий, лежащий в основе метода, может применяться как для поиска входящих аномалий (сетевых атак), так и для поиска аномалий в исходящем трафике (DLP-системы).

В [12] на основании анализа обширных экспериментальных исследований показано, что существующие модели трафика в современных сетях связи должны отражать не только самоподобные свойства, но и другие характеристики этих потоков трафика, например, мультифрактальные (МФ). Кроме того, структура этих моделей должна учи-

тываться в алгоритме прогнозирования трафика, который выигрывает от более точного моделирования трафика.

В [13] МФ-свойства трафика магистральных сетей Интернета анализируются на основе вычисления функции МФ-спектра над временны́ми рядами, сформированными из различных параметров трафика: IP-адресов и портов отправителя и получателя; временно́й метки; размера сетевого пакета; числа сетевых пакетов в потоке; типа сетевого протокола транспортного уровня; числа сетевых пакетов протоколов каждого типа; числа исходящих и входящих подключений для хоста и т. д. Данный список может быть расширен. Кроме того, выделенные значения в дальнейшем подвергаются статистической обработке для получения таких параметров, как среднее/максимальное/минимальное число пакетов, размер пакета и т. д. Все вышеописанные параметры необходимы для контроля поведения сетевого трафика; именно эти параметры формируют временны́е ряды, над которыми вычисляются МФ-эвристики.

В работах [14, 15] предложено использовать МФ-анализ для выявления в трафике магистральных сетей аномалий, свидетельствующих о сетевых неполадках или атаках. В качестве метрик безопасности применены значения характеристик МФ-спектра. Эффективность предложенного подхода подтверждена экспериментальными данными по обнаружению атак отказа в обслуживании.

Вместе с тем во всех указанных работах в качестве основных рассматривались традиционные асимптотические методы оценки ФР. Однако, используя методы текущей оценки ФР в скользящем окне в реальном масштабе времени, можно усовершенствовать рассмотренные алгоритмы.

В [16, 17] рассматривается метод обнаружения аномалий трафика на основе кратномасштабного МФ-анализа путем контроля за скачками ФР в режиме реального времени. Анализируемый метод базируется на текущей оценке МФ-свойств трафика с помощью скользящего окна и кратномасштабном вейвлет-анализе. Полученные численные данные позволяют сделать вывод, что использование ФР для различных составляющих МФ-спектра позволяют с высокой достоверностью зафиксировать наличие аномалии. Учет подобных составляющих МФ-спектра может быть реализован, например, путем построения многоканального алгоритма, каждый канал которого ориентирован на его соответствующую составляющую.

Информация о различии спектров ФР обрабатываемых процессов (если они доступны для обработки) при разном разрешении по времени может быть использована для модификации алгоритмов обнаружения/классификации КА методами машинного обучения и может привести к улучшению показателей классификации [18–21].

Целью работы являются экспериментальные оценки параметров МФ-спектра ФР компьютерных атак и нормального трафика и их информативная значимость, которые могут быть использованы как дополнительные информационные признаки при реализации алгоритмов классификации КА методами машинного обучения на примере сетей IoT.

Структура и характеристики экспериментального набора данных

В качестве примера, на котором иллюстрируется оценка МФ-характеристик анализируемого трафика, была рассмотрена база Kitsune (2019) [22–24], в которой собран набор данных сетевого трафика от устройств Интернета вещей (IoT, *аббр. от англ.* Internet of Things). Набор содержит информацию о различных типах атак, таких как разведка (Recon), человек посередине (MitM), отказ в обслуживании (DoS) и вредоносное ПО для ботнетов Mirai (Botnet Malware). В дальнейшем основное внимание уделено вредоносному ПО типа Mirai, которое заражает IoT-устройства и превращает их в сеть дистанционно управляемых ботов, называемых «зомби».

Информационные признаки (атрибуты) КА представляют собой инкрементальные (пошаговые) статистики поступающих данных. Так, если $S = \{x_1, x_2, ...\}$ представляет собой неограниченный поток данных, где $x_i \in R$ – последовательность наблюдаемых размеров пакетов, то процедура обновления кортежа для вставки x_i в IS имеет вид:

$$IS \leftarrow (N + 1, L_{S_i} + xi, SS_i + x_i^2),$$

а текущие статистики в любой момент времени:

$\mu_{S_i} = \frac{1}{N}\sum_{i=1}^{N} x_i$ – выборочное среднее;

$\sigma_{S_i}^2 = \frac{1}{N}[\sum_{i=1}^{N} x_i^2 - \mu_S^2]$ – дисперсия;

$\sigma_S = \sqrt{\sigma_S^2}$ – среднеквадратичное отклонение (СКО).

Помимо перечисленных статистик, при формировании атрибутов КА и нормального трафика список статистик, вычисляемых из инкрементальной статистики $IS_{i,\lambda}$, включал также коэффициенты ковариации $\mathrm{cov}(x_i, x_j)$ и корреляции R_{ij}, дополнительные двумерные статистики:

$$M_{ij} = \sqrt{\mu_{S_i}^2 + \mu_{S_j}^2} \text{ и } Q_{ij} = \sqrt{(\sigma_{S_i}^2)^2 + (\sigma_{S_j}^2)^2}.$$

Используя перечисленные статистики в [22, 23], после предобработки сформирован набор из 23 признаков в пяти временных окнах L = 5: 100 мс, 500 мс, 1,5 с, 10 с и 1 мин с учетом коэффициента «старения» λ = 5, 3, 1, 0,1 и 0,01.

В результате сформирован набор из 115 атрибутов (признаков), характеризующих перечисленные выше типы КА за указанные пять временных интервалов. Набор представлен в таблице 1, где атрибуты в первых 23 строках положены в основу алгоритмов обнаружения и классификации КА в сетях IoT [22, 23]. Однако результаты исследований, представленные в [24], показали, что нормальный трафик и КА в сетях IoT обладают специфичными фрактальными свойствами, что может быть дополнительно использовано для повышения эффективности обработки. В частности, показано, что скачки ФР трафика при возникновении атак могут быть использованы при создании алгоритмов обнаружения КА в сетях IoT, а численные характеристики ФР могу быть использованы в качестве дополнительных информационных признаков КА в задачах классификации методами машинного обучения.

ТАБЛИЦА 1. Набор атрибутов в данных Kitsune в разных временны́х окнах

TABLE 1. Set of Attributes in Kitsune Data in Different Time Windows

	№ атрибута	Атрибут
1	1, 24, 47, 70, 93	Длина комбинации MAC-IP в битах (μ)
2	2, 25, 48, 71, 94	Длина SrcIP в битах (μ)
3	3, 26, 49, 72, 95	Длина Channel в битах (μ)
4	4, 27, 50, 73, 96	Длина Socket в битах (μ)
5	5, 28, 51, 74, 97	Длина комбинации MAC-IP в битах (σ)
6	6, 29, 52, 75, 98	Длина SrcIP в битах (σ)
7	7, 30, 53, 76, 99	Длина Channel в битах (σ)
8	8, 31, 54, 77, 100	Длина Socket в битах (σ)
9	9, 32, 55, 78, 101	Длина Channel в битах (M_{ij})
10	10, 33, 56, 79, 102	Длина Socket в битах ($M_{ij)}$
11	11, 34, 57, 80, 103	Длина Channel в битах(Q_{ij})
12	12, 35, 58, 81, 104	Длина Socket в битах(Q_{ij})
13	13, 36, 59, 82, 105	Длина Channel в битах ($\mathrm{Cov}_{i,j}$)
14	14, 37, 60, 83, 106	Длина Socket в битах ($\mathrm{Cov}_{i,j}$)
15	15, 38, 61, 84, 107	Длина Channel в битах (R_{ij})
16	16, 39, 62, 85, 108	Длина Socket в битах (R_{ij})
17	17, 40, 63, 86, 109	Количество пакетов MAC-IP (N)
18	18, 41, 64, 87, 110	Количество пакетов SrcIP в битах (N)
19	19, 42, 65, 88, 111	Количество пакетов Channel в битах (N)
20	20, 43, 66, 89, 112	Количество пакетов Socket в битах (N)
21	21, 44, 67, 90, 113	Межпакетные задержки исходящего трафика (N)
22	22, 45, 68, 91, 114	Межпакетные задержки исходящего трафика, Channel (μ)
23	23, 46, 69, 92, 115	Межпакетные задержки исходящего трафика, Channel (σ)
24	116, 117, 118, 119, 120	МФ-спектр ФР данных в окне разрешения $\{\widehat{H}_{t_{Д_i}}, i = \overline{1,5}\}$

Фрактальный анализ компьютерных атак на примере трафика IoT

Для оценки текущих значений ФР в режиме реального времени предлагается использовать оценки ФР (показателя $\widehat{H}$) в скользящем окне, полученные методами дискретного вейвлет-анализа [17]. Рассмотрим процесс формирования оценки ФР на примере трафика IoT при воздействии атаки Mirai в скользящем окне размером Δ= 2000 отсчетов, представленного на рисунке 1а. Будем считать наблюдаемый случайный процесс $\{X(t_i), \overline{i = 1, I}\}$ дискретным. Произведем разложение трафика по вейвлет-коэффициентам в скользящем окне анализа размера Δ, смещение которого осуществляется с шагом $K \le P$. В результате при смещении окна анализа слева направо оно «пробежит» m положений $M = {}^{P}/_{K}, m = \overline{1, M}$. В результате вейвлет-коэффициенты детализации вейвлет-разложения при m-м положении окна $d_{j,k}^{m}$ могут быть найдены в конце анализируемого интервала.

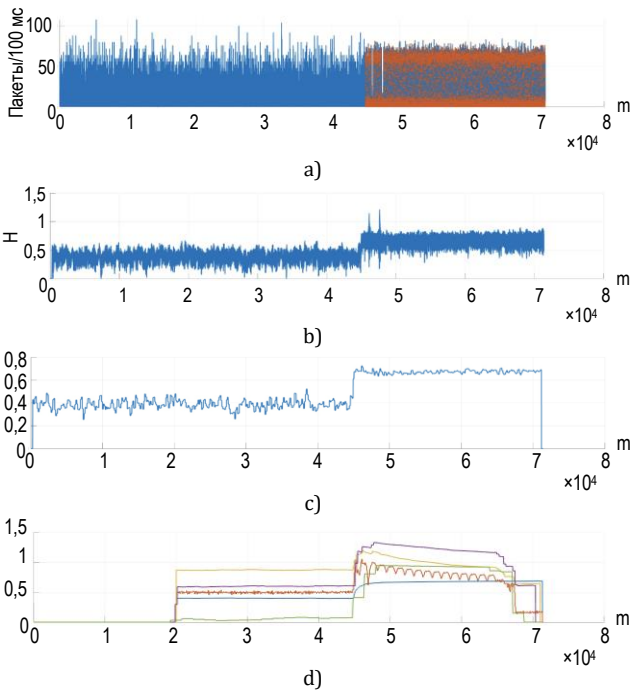

Рис. 1. Фрагмент трафика IoT при воздействии атаки Mirai (a) и оценка параметров его ФР в скользящем окне: $\widehat{H}$ с фильтрацией (b) и без фильтрации (c); МФ-спектра при $i = \overline{1,5}$ (d)

Fig. 1. A Fragment of IoT traffic under the Mirai Attack Influence (a) and Estimate of Its Fractal Dimensionality Parameters in a Sliding Window: $\widehat{H}$ with Filtering (b) and Without Filtering (c); Multifractal Spectrum at i =(1.5) (d)

Для нахождения текущей оценки параметра Херста $\widehat{H}_m$ при m-м положении окна анализа необходимо выполнить линейную регрессию на шкале j в диапазоне $[j_1, j_2]$, в соответствии с уравнением:

$$\log_2(\mu_{j,m}) = \log_2\left(\frac{1}{n_j}\sum_k \left|d_x^{(m)}(j,k)\right|^2\right) = \\ = (2\hat{H}_m - 1)j + \hat{c} = \alpha_m j + \hat{c}, \quad (1)$$

где $\hat{c} = \text{const}$.

Уравнение (1) описывает способ оценки показателя Херста $\hat{H}_m$ для процессов с долговременной зависимостью в виде линейной функции вида $\hat{a}_m = (2\hat{H}_m - 1)$.

Оценка параметра Херста в m-м положении скользящего окна $\hat{H}_m$ может быть получена путем оценки наклона графика функции $\log_2(\mu_{j,m})$ от j при каждом m-м положении окна анализа и имеет следующий вид [12]:

$$\hat{H}_m = \frac{1}{2}\left[\frac{\sum_{j=j_1}^{j_2} S_j j \eta_{j,m} - \sum_{j=j_1}^{j_2} S_j j \sum_{j=j_1}^{j_2} S_j \eta_{j,m}}{\sum_{j=j_1}^{j_2} S_j \sum_{j=j_1}^{j_2} S_j j^2 - (\sum_{j=j_1}^{j_2} S_j j^2)} + 1\right], \quad (2)$$

где $S = \sum_{j=j_1}^{j_2} 1/\sigma_j^2$, $S_1 = \sum_{j=j_1}^{j_2} j/\sigma_j^2$, $S_2 = \sum_{j=j_1}^{j_2} j^2/\sigma_j^2$ – весовые коэффициенты;

$$\sigma_j^2 = \frac{\xi\left(2, \frac{n_j}{2}\right)}{\ln^2 2} \sim \frac{2}{n_j \ln^2 2};$$

$$n_{j,m} = \log_2\left(\frac{1}{n_j}\sum_k \left|d_x^{(m)}(j,k)\right|^2\right).$$

Текущая оценка $\hat{H}_m$, полученная с помощью (2), в скользящем окне формируется с высокой дисперсией и резкими скачками показателя Херста, как это можно заметить на рисунке 1b. Для сглаживания резких выбросов и уменьшения дисперсии оценка $\hat{H}_m$ в [6] предлагается воспользоваться процедурой трешолдинга *(от англ.* Thresholding, пороговое значение), с помощью которой осуществляется дополнительная фильтрация текущих оценок показателя Херста. В результате использования трешолдинга формула для текущей оценки $\hat{H}$ с использованием дискретного вейвлет-предобразования приобретает следующий вид [6]:

$$\hat{H}(t_m) = \sum_{l=1}^{L_0} a_l^{(H)} \varphi_l^{(H)}(t_m) + \\ + \sum_{j=1}^{J}\sum_{l=1}^{L_j} T(d_{j,l}^{(H)}) \psi_{j,l}^{(H)}(t_m), \quad (3)$$

где $a_{j_0,l}^{(H)}, d_{j,l}^{(H)}$ – аппроксимирующие и детализирующие коэффициенты оценки показателя Херста при m-м положении окна фильтрации; $T(d_{j,l}^{(H)})$ – отфильтрованные с помощью преобразования трешолдинга; T(.) – детализирующие вейвлет-коэффициенты; $a_{j_0,l}^{(H)} = \left\langle \hat{H}(t_m), \phi_l^{(H)} \right\rangle$ – масштабные коэффициенты аппроксимации, равные скалярному произведению оценки показателя Херста $\hat{H}(t_m)$ и масштабной функции «самого грубого» масштаба j, смещенной на l единиц масштаба вправо от начала координат; $d_{j,l}^{(H)} = \left\langle \hat{H}(t_m), \psi_{j,l}^{(H)} \right\rangle$ – вейвлет-коэффициенты детализации масштаба j, равные скалярному произведению оценки показателя Херста $\hat{H}(t_m)$ и вейвлета масштаба j, смещенного на l единиц масштаба вправо от начала координат при $L_0 == 2^{J_{\max}}, (L_0 \le L)$, а $J_{\max} = [\log_2 L]$ – максимальное число масштабов разложения; $[\log_2 L]$ – целая часть числа.

Результаты сглаживания можно видеть на рисунке 1c.

При гауссовских и квазидекоррелированных вейвлет-коэффициентах дисперсия оценки $\hat{H}$ может быть оценена соотношением [17]:

$$\sigma_H^2 = \text{var}\hat{H}(j_1, j_2) = \frac{2}{n_{j_1} \ln^2 2} \frac{1 - 2^J}{1 - 2^{-(J+1)}(J^2+4) + 2^{-2J}}, \quad (4)$$

где $J = j_2 - j_1$ – число октав, вовлеченных в линейное сглаживание; $n_{j_1} = 2^{-j_1} N_0$ – число доступных коэффициентов в рамке j_1.

Из формулы (4) в гауссовском и асимптотическом приближении можно получить доверительный интервал:

$$\hat{H} - \sigma_{\hat{H}} z_\beta \le H \le \hat{H} + \sigma_{\hat{H}} z_\beta,$$

где z_β представляет $1 - \beta$ квантиль стандартного Гауссовского распределения, то есть $P(z \ge z_\beta) = \beta$. Все результаты, представленные ниже, и при числовом моделировании, и при фактическом анализе данных, были подсчитаны при $\beta = 0{,}025$ (т. е. 95 % доверительный интервал).

Предложенная модификация алгоритма оценки ФР (3) основана на использовании дополнительной фильтрации показателя Херста $\hat{H}$ внутри скользящего окна. Как показано в [6], для получения достоверной оценки показателя Херста целесообразно использовать вейвлеты Хаара, поскольку в этом случае наблюдается самая низкая дисперсия оценки ФР.

Оценка параметров мультифрактального спектра фрактальной размерности

Учитывая, что свойство самоподобия наблюдается в широких временны́х масштабах (например, при различном временно́м разрешении на уровне бит, пакетов, потоков и т. д.), наличие в сигнале продолжительных атак и аномальной активности изменяет самоподобную природу трафика, приводит к МФ-структуре обрабатываемых процессов [21], что может быть использовано, например, для повышения эффективности классификации КА методами машинного обучения.

С целью исследования этого феномена уточним понятие мультифрактального спектра фрактальной размерности. *Под МФ-спектром ФР будем понимать последовательность текущих оценок ФР* $\widehat{H}_{t_{Д_i}}$ *в окне анализа* Δ *фиксированной длины в зависимости от интервала разрешения* (времени дискретизации $t_Д$):

$$\{\widehat{H}_{t_{Д_i}} = f\left(t_{Д_i}\right);\ i = \overline{1,L};\ t_{Д_i} \in \Delta;\ \Delta = \text{const}\}. \quad (5)$$

Исследования показывают, что анализируемый случайный процесс в сети IoT можно считать мультифрактальным, поскольку при разных временны́х шкалах (при разном временно́м разрешении) величина ФР изменяется. В общем случае оценка ФР является случайной величиной $\widehat{H} \in N(m_{\widehat{H}}, \sigma^2_H)$ и полно характеризуется моментами распределения – средним значением $m_{\widehat{H}}$ и дисперсией σ^2_H оценки.

Для оценки характеристик МФ-спектра ФР рассматриваемых процессов в сетях IoT в виде (5) были выбраны следующие параметры:

– окно оценки ФР Δ = 2000 отсчетов;

– количество окон $L = 5$, так что $i = \overline{1,5}$;

– время дискретизации наблюдаемых процессов в анализируемых пяти окнах: $t_{Д_1}$ = 100 мс, $t_{Д_2}$ = = 500 мс, $t_{Д_3} = 1$ с, $t_{Д_4} = 2$ с, $t_{Д_5} = 10$ с.

По итогам исследования были получены значения МФ-спектра ФР для нормального трафика в разных точках описанной топологии сети IoT и разных типов КА типа Mirai, что иллюстрируется на рисунке 1d. В таблице 2 приведены статистические характеристики оценок показателя Херста $\widehat{H}$ в скользящем окне с применением процедуры трешолдинга для пяти окон оценивания размером 100 мс, 500 мс, 1,5 с, 10 с и 1 мин, соответственно.

Количественный анализ полученных результатов показывает, что в отсутствии КА трафик IoT характеризуется оценками среднего значения $m_{\widehat{H}}$ в интервале {0…0,5} для интервалов дискретизации: $t_{Д_1}$ = 100 мс, $t_{Д_4}$ = 2 с, $t_{Д_5}$ = 10 с. Это означает, что анализируемый случайный процесс при этих интервалах дискретизации не обладает самоподобием. При $t_{Д_2}$ = 500 мс и $t_{Д_3}$ = 1 с значение $m_{\widehat{H}}$ лежит в диапазоне {0,5…1,0}, что свидетельствует о наличии фрактальных свойств у нормального трафика при этом временно́м разрешении.

Для КА типа Mirai фрактальными свойствами атака обладает при $t_{Д_1}$ = 100 мс, $t_{Д_2}$ = 500 мс, $t_{Д_5}$ = 10 с. В этом случае значение $m_{\widehat{H}}$ лежит в диапазоне {0,5…1,0}, что свидетельствует о наличии у КА фрактальных свойств при этом временно́м разрешении. При $t_{Д_3}$ = 1 с, $t_{Д_4}$ = 2 с параметр $m_{\widehat{H}} > 1$, что указывает на наличие аномалий или на нестационарность обрабатываемого процесса.

Указанные значения ФР могут быть использованы в качестве дополнительных атрибутов алгоритма обнаружения атак в сетях IoT для атаки Mirai. На рисунке 2 показаны $\widehat{m_{\widehat{H}}}$ и СКО оценок в скользящем окне Δ при различном временно́м разрешении. Величина $\widehat{H}$ обычно характеризует степень самоподобия процесса следующим образом. Случай 0,5 < H < 1,0 характеризует трендоустойчивый, обладающий длительной памятью процесс, который является самоподобным; 0 < H < 0,5 – характерен для случайного процесса, не обладающего самоподобием; H > 1,0 – ссоответствует аномалии (нестационарности) анализируемого процесса.

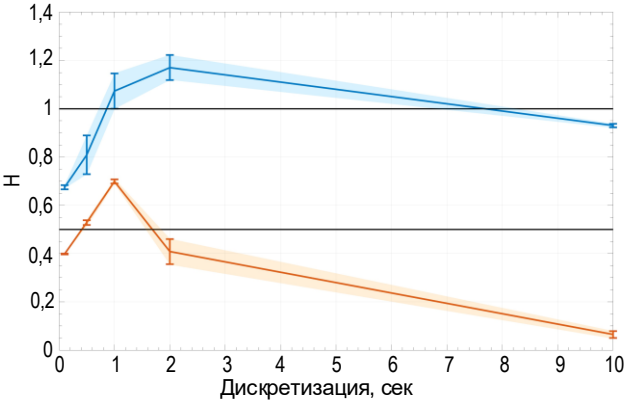

Рис. 2. Оценка показателя Херста при атаке Mirai (синим) и нормального трафика (оранжевым) без аномальных выбросов при разном временном разрешении

Fig. 2. Hurst Exponent Evaluation on Mirai Attack (blue) and Normal Traffic (orange), Filtered Evaluation without Anomalous Outliers at Different Time Resolutions

Используя численные значения среднего $m_{\widehat{H}}$ и СКО фрактальной размерности $\sigma_{\widehat{H}}$ нормального трафика и КА, представленные в таблице 2, предлагается добавить к уже имеющимся атрибутам значения МФ-спектра ФР нормального трафика. Для КА типа атаки Mirai эти пять элементов, характеризующих $\{\widehat{H}_{t_{Д_i}}, i = \overline{1,5}\}$, представлены в строке 24 таблицы 1. В результате количество атрибутов для нормального трафика и КА типа Mirai увеличивается до 120.

ТАБЛИЦА 2. Статистические характеристики оценки нормального / КА трафика IoT с трешолдингом

TABLE 2. Statistical Characteristics of Normal / CA IoT Traffic Assessment with Thresholding

$t_{Д_i}$	$m_{\widehat{H}}$	$\sigma^2_{\widehat{H}}$	$\sigma_{\widehat{H}}$
100 мс	0,3983 / 0,6745	0,00003 / 0,000075	0,0019 / 0,0087
500 мс	0,5285 / 0,8089	0,00096 / 0,0065	0,0098 / 0,0804
1 с	0,6987 / 1,073	0,000069 / 0,0054	0,0084 / 0,0732
2 с	0,4080 / 1,1703	0,0027 / 0,0027	0,0522 / 0,052
10 с	0,0646 / 0,9303	0,0002 / 0,0004	0,0143 / 0,007

Информативная значимость атрибутов

Для оценки влияния на качество классификации КА введенных дополнительных параметров МФ-спектра ФР была оценена их информационная значимость в случае бинарной и многоклассовой классификации. Результаты оценки по индексу Джини без добавления и с добавлением МФ-спектра ФР приведены в виде гистограмм на рисунке 3. Оценка информативности проводилась относительно классовых меток о наличии (отсутствии) КА типа Mirai Botnet.

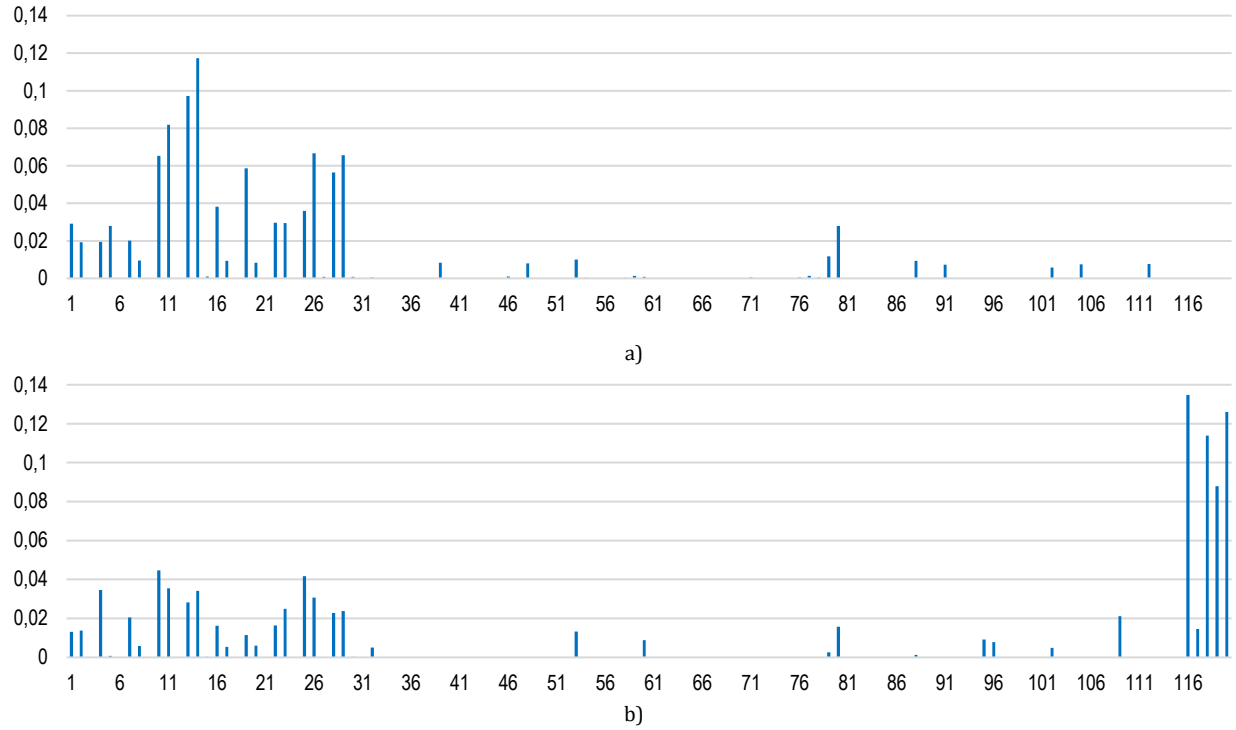

Рис. 3. Оценка информативной значимости атрибутов в задаче бинарной классификации КА типа Mirai Botnet по индексу Джини для двух случаев: без добавления (a) и с добавлением МФ-спектра ФР (b)

Fig. 3. Assessment of the Informative Significance of Attributes in the Task of Binary Classification of the Mirai Botnet Spacecraft Using the Gini Index for Two Cases: a) without Adding Multifractal Spectrum Characteristics of Fractal Dimension (MSFD); b) with the Addition of MSFD

Для сопоставления размерности гистограмм в первом случае оценка важности по представленным в таблице 1 атрибутам 116–120 присвоена равной 0. Был проведен анализ первых 15 наиболее значимых атрибутов для двух случаев – без добавления и с добавлением МФ-спектра ФР.

Анализ распределения на рисунке 3а показал, что наиболее информативными являются атрибуты компьютерной сети (КС), полученные во временно́м окне 100 мс (см. таблицу 2) и λ = 5. В число первых 15 наиболее значимых атрибутов, вычисленных для случая без добавления МФ-спектра ФР, попало: 10 – вычисленных во временно́м окне 100 мс; 4 – 500 мс; 1 атрибут – 10 с. Анализ наиболее значимых атрибутов выявил только 2 «дублирования» по разным временным окнам (атрибуты № 5 и 28 – σ длин комбинаций MAC-IP в битах и атрибуты № 11 и 80, дисперсия длины Channel в битах), в остальном все значимые атрибуты уникальны и не пересекаются.

«Концентрация» наиболее значимых атрибутов в области λ = 5 может быть обусловлена возможностью детектирования КА во временно́м окне 100 мс. Атрибуты, вычисленные в других временны́х окнах, являются вспомогательными. Добавление МФ-спектра ФР в атрибутное пространство изменяет распределение его информационной значимости по оси ординат (атрибуты 1 … 115 снизили значимость, в среднем, на 50 %, однако их ранжирование практически не претерпело изменений).

Анализ 15 наиболее значимых атрибутов с учетом добавления МФ-спектра ФР показал, что 6 из 15 атрибутов (40 %) – уникальны. В их число включается 4 атрибута, связанных с МФ-спектром ФР. 7 атрибутов из 15 вычислены во временно́м окне 100 мс. Четыре атрибута – вычислены для временного окна 500 мс. Один атрибут вычислен для временного окна 1.5 с, один – для временного окна 2 с, и 2 атрибута – для временного окна 10 с.

Анализ атрибутов № 116 … 120, связанных с МФ-спектром ФР, демонстрирует корреляцию, близкую к линейной, между МФ-спектром ФР и классовыми метками о наличии (отсутствии) КА типа Mirai Botnet. Столь высокая корреляция обусловлена тем, что во время проведения КА типа Mirai Botnet ряд атрибутов КС, связанных с сете-

вым взаимодействием (в таблице 2, атрибуты № 10, 11, 13 и 14, связаны с количеством исходящих пакетов), резко меняют свое распределение (количество пакетов резко возрастает). Таким образом, добавление МФ-спектра ФР в атрибутное пространство изменяет распределение его информационной значимости по оси ординат.

Так, атрибуты 1…115 снизили значимость, в среднем на 50 %, однако их ранжирование практически не претерпело изменений. Оценка информативности атрибутов в задаче многоклассовой классификации КА типов Mirai Botnet и OS Scan по критерию Джини представлена на рисунке 4.

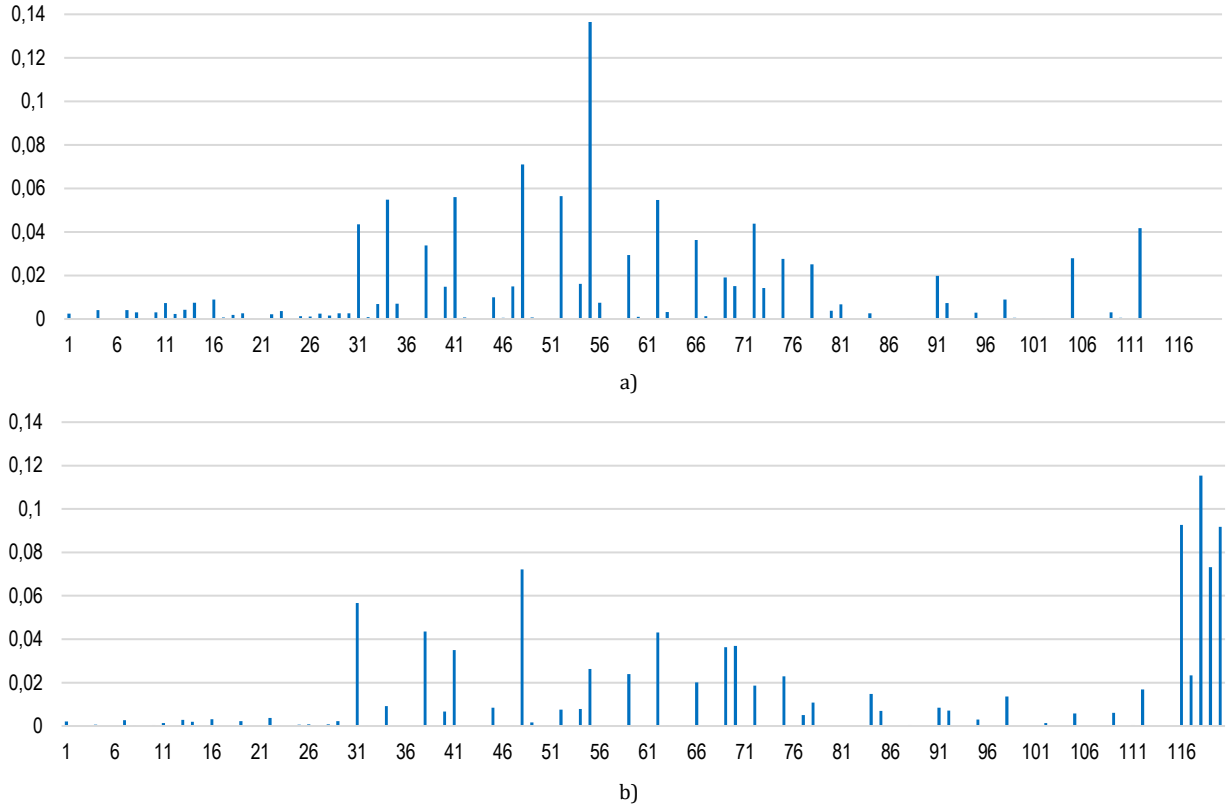

Рис. 4. Оценка информативной значимости атрибутов в задаче многоклассовой классификации КА типов Mirai Botnet и OS Scan по критерию Джини для двух случаев без добавления (а) и с добавлением ФР (б)

Fig. 4. Assessment of the Informative Significance of Attributes in the Task of Multi-Class Classification of the Mirai Botnet and OS Scan Spacecraft Using the Gini Criterion for Two Cases: a) without Adding Fractal Dimension; b) with the Addition of Fractal Dimension

В сравнении с рисунком 3 из данных, представленных на рисунке 4, видно, что распределение атрибутного пространства «сдвинуто» в сторону более широкого временного окна 500 мс (атрибуты с 24 по 46) и 1,5 с (атрибуты с 47 по 69).

Аналогично случаю бинарной классификации, был проведен анализ первых 15 наиболее значимых атрибутов для двух случаев – без добавления и с добавлением МФ-спектра ФР.

В число первых 15 наиболее значимых атрибутов, вычисленных для случая без добавления МФ-спектра ФР, не попало ни одного атрибута, вычисленного для временно́го окна в 100 мс. Основная концентрация атрибутов наблюдается на интервале 500 мс…1,5 с и составляет 67 %, остальные атрибуты распределены в диапазоне 2…10с. «Сдвиг» информационной значимости атрибутов в область более широких временны́х окон может быть обусловлен наличием атаки второго типа – OS Scan, а также большого количества данных о нормальном функционировании КС. С учетом объединения наборов данных (для КА типов Mirai Botnet и OS Scan) доля «нормальных» записей в итоговом наборе составляет 92 % (2 274 666 шт.) против 84 % (642 516 шт.) в исходном наборе данных Mirai Botnet.

При классификации двух КА в условиях усилившегося дисбаланса классов, временно́е окно в 100 мс не является достаточно информативным. Больше информации может быть извлечено из атрибутов, полученных на временны́х окнах от 500 мс и выше.

Анализ 15 наиболее значимых атрибутов с учетом добавления МФ-спектра ФР позволил сделать выводы, схожие со случаем бинарной классификации. Семь из 15 атрибутов (47 %) – уникальны. В

их число входят 5 атрибутов (против 4 атрибутов в случае бинарной классификации), связанных с МФ-спектром ФР. Линейная корреляция между последним и классовыми метками о наличии или отсутствии КА типа Mirai Botnet сохраняется.

Таким образом, добавление фрактальной размерности КА типа Mirai Botnet в атрибутное пространство изменяет распределение информативности атрибутов аналогично эксперименту с бинарной классификацией. Изменение по оси ординат не столь выраженно, поскольку фрактальная размерность добавлена только для КА типа Mirai Botnet.

Заключение

Введено понятие МФ-спектра ФР в виде последовательности текущих оценок ФР $\widehat{H}_{t_{Д_i}}$ в окне анализа фиксированной длины в зависимости от интервала разрешения.

Найденные экспериментальные значения параметров МФ-спектра ФР, представленные в виде дополнительных атрибутов в таблице 1 (атрибуты № 116…120), представляющих собой текущие оценки ФР $\widehat{H}_{t_{Д_i}}$ в окне анализа для различных интервалов разрешения.

Полученные дополнительные атрибуты нормального трафика и трафика под КА, а также распределения их информационной значимости могут быть использованы для повышения достоверности обнаружения и эффективности классификации КА методами машинного обучения в сетях IoT, как это показано в [25].

Для задачи бинарной классификации КА типа Mirai Botnet для двух случаев: без добавления и с добавлением МФ-спектра ФР, – получена оценка информативной значимости атрибутов по индексу Джини. Показано, что наиболее информативными являются атрибуты КС, полученные во временно́м окне 100 мс.

Добавление МФ-спектра ФР в атрибутное пространство изменяет распределение его информационной значимости. Атрибуты № 116…120, связанные с МФ-спектром ФР, демонстрируют корреляцию, близкую к линейной, между МФ-спектром ФР и классовыми метками о наличии (отсутствии) КА типа Mirai Botnet.

Показано, что основная концентрация наиболее значимых атрибутов приходится на интервал 500 мс … 1,5 с (67 %), остальные распределены в диапазоне 2…10 с. «Сдвиг» информационной значимости атрибутов в область более широких временны́х окон обусловлен наличием атаки второго типа – OS Scan, а также большого количества данных о нормальном функционировании КС.

Список источников

1. Park K., Willinger W. Self-Similar Network Traffic: An Overview // In: Self-Similar Network Traffic and Performance Evaluation. John Wiley & Sons, 2000. DOI:10.1002/047120644X.ch1

2. Шелухин О.И., Осин А.В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. М: Физматлит, 2008. С. 362. EDN:MVSWAB

3. Sheluhin O., Smolskiy S., Osin A. Self-Similar Processes in Telecommunications. John Wiley & Sons, 2007. 334 p.

4. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. М: Горячая линия – Телеком, 2019. С. 448.

5. Sheluhin O., Kazhemskiy M. Influence Of Fractal Dimension Statistical Charachteristics On Quality Of Network Attacks Binary Classification // Proceedings of the 28th Conference of Open Innovations Association (FRUCT, Moscow, Russia, 27–29 January 2021). Vol. 28. IEEE, 2021. PP. 407–413. DOI:10.23919/FRUCT50888.2021.9347600. EDN:XMLZKW

6. Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode // Proceedings of the 28th Conference at Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF, St. Petersburg, Russia, 30 May 2022 – 03 June 2022). Vol. 5. IEEE, 2022. PP. 430–435. DOI:10.1109/WECONF55058.2022.9803635. EDN:UEYFUM

7. Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Влияние фрактальной размерности на качество классификации компьютерных атак методами машинного обучения // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 1. С. 57–64. DOI:10.36724/2409-5419-2023-15-1-57-64. EDN:EVELAW

8. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6(98). С. 64–71. DOI:10.22184/2070-8963.2021.98.6.64.70. EDN:KRIUAD

9. Перов Р.А., Лаута О.С., Крибель А.М., Федулов Ю.М. Комплексная методика обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 2. С. 44–51. DOI:10.36724/2409-5419-2022-14-2-44-51. EDN:ELALFA

10. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения // Информатика и автоматизация. 2022. Т. 21. № 6. С. 1328–1358. DOI:10.15622/ia.21.6.9. EDN:IWILXQ

11. Карачанская Е.В., Соседова Н.И. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре // Безопасность информационных технологий. 2019. Т. 26 № 1. С. 98–110. EDN:YZELNB

12. Vieira F.H.T., Bianchi G.R., Lee L.L. A Network Traffic Prediction Approach Based on Multifractal Modeling // Journal of High Speed Networks. 2010. Vol. 17(2). PP. 83–96. DOI:10.3233/JHS-2010-0334

13. Зегжда П.Д, Лаврова Д.С., Штыркина А.А. Мультифрактальный анализ трафика магистральных сетей интернет для обнаружения атак отказа в обслуживании // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 48–58. EDN:XTKTFZ

14. Лаврова Д.С., Зегжда Д.П., Зегжда П.Д., Штыркина А.А. Оценка киберустойчивости информационно-технологических систем на основе самоподобия // Материалы 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Изд-во Политехн. Ун-та, 2016. С. 101–104. EDN:YPUWMH

15. Штыркина А.А., Зегжда П.Д, Лаврова Д.С. Обнаружение аномалий в трафике магистральных сетей Интернет с использованием мультифрактального анализа // Материалы 27-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Изд-во Политехн. Ун-та, 2018. С. 14–15. EDN:YPUXQD

16. Шелухин О.И., Панкрушин А.В. Обнаружение аномальных выбросов в реальном масштабе времени методами мультифрактального анализа // Нелинейный мир. 2016. Т. 14. № 2. С. 72–82. EDN:VTZNTH

17. Sheluhin O.I., Lukin I.Y. Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode // Automatic Control and Computer Sciences. 2018. Vol. 52. Iss. 5. PP. 421–430. DOI:10.3103/S0146411618 050115. EDN:OJQHKD

18. Riedi R.H., Crouse M.S., Ribeiro V.J., Baraniuk R. A multifractal wavelet model with application to network traffic // IEEE Transactions on Information Theory. 1999. Vol. 45. Iss. 3. PP. 992–1018. DOI:10.1109/18.761337

19. Taqqu M.S., Teverovsky V., Willinger W. Is Network Traffic Self-Similar or Multifractal? // Fractals. 1997. Vol. 5. PP. 63–73. DOI:10.1142/S0218348X97000073

20. Sheluhin O.I., Garmashev A.B., Aderemi A.A. Detection of teletraffic anomalies using multifractal analysis // International Journal of Advancements in Computing Technology. 2011. Vol. 3. Iss. 4. PP. 174–182. DOI:10.4156/ijact.vol3.issue4.19. EDN:PDYTSP

21. Шелухин О.И. Мультифракталы: инфокоммуникационные приложения. М.: Горячая линия – Телеком, 2011. 576 с. EDN:QMUYXJ

22. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: an Ensemble of Autoencoders for Online Network Intrusion Detection // arXiv:1802.09089v2. 2018. DOI:10.48550/arXiv.1802.09089

23. Miyamoto K., Goto H., Ishibashi R., Han C., Ban T., Takahashi T., et al. Malicious Packet Classification Based on Neural Network Using Kitsune Features // Proceedings of the 2nd International Conference on Intelligent Systems and Pattern Recognition (ISPR 2022, Hammamet, Tunisia, 24–26 March 2022). Communications in Computer and Information Science. Vol. 1589. Cham: Springer, 2022. PP. 306–314. DOI:10.1007/978-3-031-08277-1_25

24. Шелухин О.И., Рыбаков С.Ю. Статистические характеристики фрактальной размерности трафика IoT на примере набора данных Kitsune // Труды учебных заведений связи. 2023. Т. 9. № 5. С. 112–119. DOI:10.31854/1813-324X-2023-9-5-112-119. EDN:YMSJRF

25. Шелухин О.И., Рыбаков С.Ю., Раковский Д.И. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности // Вопросы кибербезопасности. 2024. № 2(60) С.107–119. DOI:10.21681/2311-3456-2024-2-107-119. EDN:GKOSBB

References

1. Park K., Willinger W. Self-Similar Network Traffic: An Overview. *In: Self-Similar Network Traffic and Performance Evaluation*. John Wiley & Sons, 2000. DOI:10.1002/047120644X.ch1

2. Sheluhin O.I., Osin A.V., Smolskiy S.M. *Self-Similarity and Fractals. Telecommunication Applications.* Moscow: Fizmatlit Publ.; 2008. 362 p. (in Russ.) EDN:MVSWAB

3. Sheluhin O., Smolskiy S., Osin A. *Self-Similar Processes in Telecommunications*. John Wiley & Sons, 2007. 334 p.

4. Sheluhin O.I. *Network Anomalies. Detection, Localization, Forecasting*. Moscow: Goryachaya liniya –Telekom Publ.; 2019. 448 p. (in Russ.)

5. Sheluhin O., Kazhemskiy M. Influence Of Fractal Dimension Statistical Charachteristics On Quality Of Network Attacks Binary Classification. *Proceedings of the 28th Conference of Open Innovations Association, FRUCT, 27–29 January 2021, Moscow, Russia, vol.28*. IEEE; 2021. p.407–413. DOI:10.23919/FRUCT50888.2021.9347600. EDN:XMLZKW

6. Sheluhin O.I., Rybakov S.Y., Vanyushina A.V. Detection of Network Anomalies with the Method of Fixing Jumps of the Fractal Dimension in the Online Mode. *Proceedings of the 28th Conference at Wave Electronics and Its Application in Information and Telecommunication Systems, WECONF, 30 May 2022 – 03 June 2022, St. Petersburg, Russia. vol.5*. IEEE; 2022. p.430–435. DOI:10.1109/WECONF55058.2022.9803635. EDN:UEYFUM

7. Sheluhin O.I., Rybakov S.Yu., Vanyushina A.V. Influence of fractal dimension on quality classification of computer attacks by machine learning methods. *H&ES Reserch*. 2023;15(1):57–64. (in Russ.) DOI:10.36724/2409-5419-2023-15-1-57-64. EDN:EVELAW

8. Kotenko I., Saenko I., Lauta O., Kribel A. The method of early detection of cyber attacks based on the integration of fractal analysis and statistical methods. *Pervaya milya*. 2021;6(98):64–71. DOI:10.22184/2070-8963.2021.98.6.64.70. EDN:KRIUAD

9. Perov R.A., Lauta O.S., Kribel A.M., Fedulov Yu.M. A comprehensive technique for detecting cyber attacks based on the integration of fractal analysis and statistical methods. *H&ES Reserch.* 2022;14(2):44–51. (in Russ.) DOI:10.36724/2409-5419-2022-14-2-44-51. EDN:ELALFA

10. Kotenko I., Saenko I., Lauta O., Kribel A. Anomaly and cyber attack detection technique based on the integration of fractal analysis and machine learning methods. *Informatics and Automation*. 2022;6(21):1328–1358. (in Russ.) DOI:10.15622/ ia.21.6.9. EDN:IWILXQ

11. Karachanskaya E.V., Sosedova N.I. Method for detection of network traffic anomalies which is based on its self-similar traffic structure. *Bezopasnost informacionnyh tehnology.* 2019;26(1):98–110. (in Russ.) EDN: YZELNB

12. Vieira F.H.T., Bianchi G.R., Lee L.L. A Network Traffic Prediction Approach Based on Multifractal Modeling. *Journal of High Speed Networks*. 2010;17(2):83–96. DOI:10.3233/JHS-2010-0334

13. Zegzhda P.D., Lavrova D.S., Shtyrkina A.A. Multifractal Analysis of Backbone Network Traffic for Denial-of-Service Attacks Detection. *Information Security Problems. Computer Systems.* 2018;2:48–58. (in Russ.) EDN:XTKTFZ

14. Lavrova D.S., Zegzhda D.P., Zegzhda P.D., Shtyrkina A.A. Assessment of cyber resilience of information technology systems based on self-similarity. *Proceedings of the 25th Scientific and Technical Conference on Methods and Technical Means of Ensuring Information Security.* St Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2016. p.101–104. (in Russ.) EDN:YPUWMH

15. Shtyrkina A.A. Zegzhda P.D., Lavrova D.S. Detecting anomalies in Internet backbone traffic using multifractal analysis. *Proceedings of the 27th Scientific and Technical Conference on Methods and Technical Means of Ensuring Information Security.* St Petersburg: Peter the Great St. Petersburg Polytechnic University Publ.; 2018. p.14–15. (in Russ.) EDN:YPUXQD

16. Sheluhin O.I., Pankrushin A.V. Detection of Anomalies in Real Time Using the Methods of Multifractal Analysis. *Nonlinear World*. 2016;14(2):72–82. (in Russ.) EDN:VTZNTH

17. Sheluhin O.I., Lukin I.Y. Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode. *Automatic Control and Computer Sciences.* 2018;52(5):421–430. DOI:10.3103/S0146411618050115. EDN:OJQHKD

18. Riedi R.H., Crouse M.S., Ribeiro V.J., Baraniuk R. A multifractal wavelet model with application to network traffic. *IEEE Transactions on Information Theory*. 1999;45(3):992–1018. DOI:10.1109/18.761337

19. Taqqu M.S., Teverovsky V., Willinger W. Is Network Traffic Self-Similar or Multifractal? *Fractals*. 1997;5:63–73. DOI:10.1142/S0218348X97000073

20. Sheluhin O.I., Garmashev A.B., Aderemi A.A. Detection of teletraffic anomalies using multifractal analysis. *International Journal of Advancements in Computing Technology.* 2011;3(4):174–182. DOI:10.4156/ijact.vol3.issue4.19. EDN:PDYTSP

21. Sheluhin O.I. *Multifractals: Infocommunication Applications*. Moscow: Goryachaya liniya –Telekom Publ.; 2011. 576 p. EDN:QMUYXJ

22. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: an Ensemble of Autoencoders for Online Network Intrusion Detection. *arXiv:1802.09089v2*. 2018. DOI:10.48550/arXiv.1802.09089

23. Miyamoto K., Goto H., Ishibashi R., Han C., Ban T., Takahashi T., et al. Malicious Packet Classification Based on Neural Network Using Kitsune Features. *Proceedings of the 2nd International Conference on Intelligent Systems and Pattern Recognition, ISPR 2022, 24–26 March 2022, Hammamet, Tunisia. Communications in Computer and Information Science, vol.1589*. Cham: Springer; 2022. p.306–314. DOI:10.1007/978-3-031-08277-1_25

24. Sheluhin O., Rybakov S. IoT Traffic Fractal Dimension Statistical Characteristics on the Kitsune Dataset Example. *Proceedings of Telecommunication Universities.* 2023;9(5):112–119. (in Russ.) DOI:10.31854/1813-324X-2023-9-5-112-119. EDN:YMSJRF

25. Sheluhin O.I., Rybakov S.Yu., Rakovsky D.I. Classification of computer attacks using multifractal spectrum of fractal dimension. *Voprosy kiberbezopasnosti*. 2024;2(60):107–119. (in Russ.) DOI:10.21681/2311-3456-2024-2-107-119. EDN:GKOSBB

Статья поступила в редакцию 08.04.2024; одобрена после рецензирования 14.04.2024; принята к публикации 03.06.2024.
The article was submitted 08.04.2024; approved after reviewing 14.04.2024; accepted for publication 03.06.2024.

Информация об авторах:

ШЕЛУХИН Олег Иванович — доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность» Московского технического университета связи и информатики
https://orcid.org/0000-0001-7564-6744

РЫБАКОВ Сергей Юрьевич — руководитель НОЦ «Информационная безопасность» Московского технического университета связи и информатики
https://orcid.org/0000-0002-4593-9009

ВАНЮШИНА Анна Вячеславовна — кандидат технических наук, доцент, доцент кафедры «Информационная безопасность» Московского технического университета связи и информатики
https://orcid.org/0000-0001-8729-6729

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.