Научная статья
УДК 519.61+539.1
DOI:10.31854/1813-324X-2023-9-5-112-119

Статистические характеристики фрактальной размерности трафика IoT на примере набора данных Kitsune

Олег Иванович Шелухин, sheluhin@mail.ru
Сергей Юрьевич Рыбаков ✉, s.i.rybakov@mtuci.ru

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

Аннотация: *В работе рассмотрен метод оценки фрактальных свойств трафика, а также проведена оценка статистических параметров фрактальной размерности (ФР) трафика IoT. Анализ реального трафика с атаками из дампа Kitsune и проведенный анализ фрактальных свойств трафика в нормальном режиме и при воздействии атак типа SSDP Flood, Mirai, OS Scan показал, что скачки ФР трафика при возникновении атак могут быть использованы при создании алгоритмов обнаружения компьютерных атак в сетях IoT. Исследования показали, что в случае онлайн-анализа сетевого трафика при оценке ФР следует отдать предпочтение модифицированному алгоритму оценки показателя Херста в скользящем окне анализа.*

Ключевые слова: показатель Херста, фрактальная размерность, трешолдинг, компьютерная атака, сетевой трафик, интернет вещей

Ссылка для цитирования: 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

IoT Traffic Fractal Dimension Statistical Characteristics on the Kitsune Dataset Example

Oleg Shelukhin, sheluhin@mail.ru
Sergey Rybakov ✉, s.i.rybakov@mtuci.ru

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

Abstract: *The paper considers a method for estimating the fractal properties of traffic, and also evaluates the statistical parameters of the fractal dimension of IoT traffic. An analysis of real traffic with attacks from the Kitsune dump and an analysis of the fractal properties of traffic in normal mode and under the influence of attacks such as SSDP Flood, Mirai, OS Scan showed that jumps in the fractal dimension of traffic when attacks occur can be used to create algorithms for detecting computer attacks in IoT networks. Studies have shown that in the case of online analysis of network traffic, when assessing the RF, preference should be given to the modified algorithm for estimating the Hurst exponent in a sliding analysis window.*

Keywords: Hurst exponent, fractal dimension, thresholding, computer attack, network traffic, internet of things

For citation: Shelukhin O., Rybakov S. IoT Traffic Fractal Dimension Statistical Characteristics on the Kitsune Dataset Example. *Proceedings of Telecommun. Univ.* 2023; 9(5):112–119. DOI:10.31854/1813-324X-2023-9-5-112-119

Введение

Технологии интернета вещей (IoT, *аббр. от англ.* Internet of Things) появились сравнительно недавно и за последнее десятилетие получили широкое распространение. IoT представляет собой систему взаимосвязанных компьютерных сетей и физических объектов, оборудованных множеством встроенных сенсоров, которые собирают информацию об окружающей среде. С этой целью используется специальное программное обеспечение, которое обрабатывает данные и передает информацию с датчиков по сети для последующего анализа, удаленного контроля и управления объектами IoT без участия пользователя. Также программное обеспечение обеспечивает функции хранения данных и обеспечивает доступ к ним [1, 2]. Обычно в рамках IoT присутствуют отдельные сети, каждая из которых разработана для решения конкретных задач.

Специалисты в области IoT прогнозируют ежегодное увеличение на 20 % количества «умных» устройств в период с 2020 по 2025 гг. [3]. В связи с быстрым ростом количества устройств и развитием технологии в целом появляются риски, связанные с обеспечением информационной безопасности. Устройства IoT («умные» бытовые приборы с доступом в интернет) подключены к интернету, связаны между собой и нередко становятся целью злоумышленников, желающих получить доступ к ресурсам «умных» устройств.

Поскольку устройства IoT обладают ограниченным объемом памяти и малой вычислительной мощностью, в них обычно не устанавливаются средства обеспечения безопасности от сетевых атак. Однако производители услуг и оборудования, связанных с IoT, чаще всего не придерживаются принципа сквозной информационной безопасности в основном из-за экономических факторов. Это означает, что информационной безопасности в сфере IoT обычно не уделяется должного внимания, несмотря на то, что все больше пользователей и организаций приобретают «умные» устройства: роутеры, камеры видеонаблюдения и др. К сожалению, мало кто задумывается о защите этих устройств и установке актуальных обновлений.

Существует опасность, связанная с распространением целевых кибератак на устройства IoT, и количество таких атак продолжает расти [4]. Злоумышленники, в частности, используют зараженные сети «умных» устройств для осуществления DDoS-атак или в качестве прокси-серверов для других вредоносных действий. Поэтому решения вопросов информационной безопасности должны учитываться и закладываться еще на стадии проектирования устройства или услуги, и поддерживаться на протяжении всего их жизненного цикла.

Согласно предоставленным данным [5], атаки на устройства IoT обычно не требуют сложной реализации, однако они достаточно незаметны для обычных пользователей. Одним из самых распространенных видов вредоносных программ, позволяющих ботнетам захватывать и управлять устройствами IoT путем использования устаревших уязвимостей, является Mirai. Например, одна из версий вредоносной сети Mirai проникла в более чем 5 миллионов устройств, включая устройства IoT, в 164 странах мира. Это семейство вредоносного программного обеспечения использовалось в 39 % всех атак. К числу других наиболее распространенных атак в сетях IoT относятся атаки типа SSDP Flood, OS Scan.

Постановка задачи

Одним из важных параметров сетевого трафика, который может быть положен в основу создания средства обеспечения безопасности от сетевых атак IoT, являются характеристики его фрактальных свойств. Известно, что сетевой трафик обладает свойствами самоподобия или фрактальными свойствами [6, 7]. Для количественной оценки фрактальных свойств трафика в основном используется показатель Херста H, который связан с фрактальной размерностью (ФР) D следующим соотношением: $D = 2 - H$.

В работах [8–10] было показано, что на основе показателя Херста можно обнаружить аномальную активность сетевого трафика, которая может характеризоваться следующими статистическими характеристиками:

1) выборочное среднее:

$$M_{H,i} = \frac{1}{n}\sum_{j=i}^{i+n} s_j ,$$

где s_j – выборочное значение оценки показателя Херста трафика в момент t_j;

2) выборочная дисперсия:

$$D_{H,i} = \frac{1}{n-1}\sum_{j=i}^{i+n}(s_j - M_{H,i})^2;$$

3) коэффициент асимметрии, определяющий степень асимметричности плотности вероятности распределения показателя Херста относительно оси, проходящей через центр ее тяжести:

$$\gamma_{H1,i} = \frac{\frac{1}{n-1}\sum_{j=i}^{i+n}(s_j - M_{H,i})^2}{D_{H,i}};$$

4) коэффициент эксцесса, демонстрирующий, насколько острую вершину имеет плотность распределения вероятности показателя Херста по сравнению с нормальным распределением:

$$\gamma_{H2,i} = \frac{\frac{1}{n-1}\sum_{j=i}^{i+n}(s_j - M_{H,i})^4}{D^2{}_{H,i}} - 3.$$

Данные параметры могут быть положены в основу построения эффективной системы сетевой защиты на базе интеллектуального анализа данных [11, 12] и методов фрактального анализа.

Целью работы является исследование статистических характеристик ФР наиболее распространенных атак в сети IoT на примере анализа базы данных Kitsune.

База данных

Оценку статистических параметров ФР трафика IoT будем проводить на основе выгрузки данных сетевого трафика базы Kitsune [13–15]. Kitsune – это сетевая система обнаружения вторжений (NIDS, *аббр. от англ.* Network Intrusion Detection System) на основе искусственной нейронной сети (ANN, *аббр. от англ.* Artificial Neural Network), работающей онлайн в автоматическом режиме.

На рисунке 1 представлена топология сети, на основе которой осуществлялся захват сетевого трафика на маршрутизаторах в точках 1, 2, 3 и *X*. Для каждого набора данных вначале захватывался чистый трафик для первого миллиона пакетов, а затем проводилась атака. На иллюстрации также указаны векторы атак.

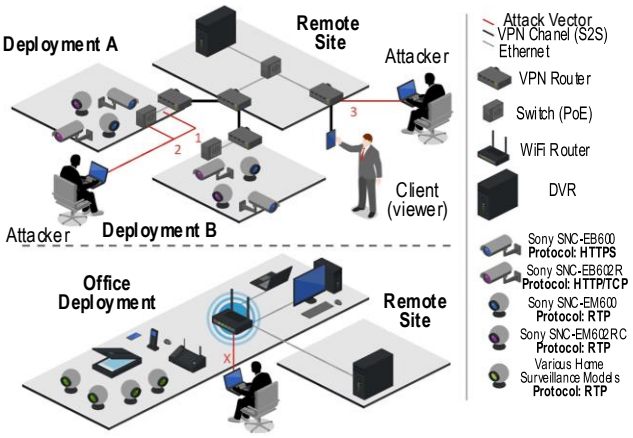


Рис. 1. Топология сети [13]

Fig. 1. Network Topology [13]

Структура извлечения объектов, называемая AfterImage, эффективно отслеживает шаблоны каждого сетевого канала, используя затухающие инкрементные статистические данные, и извлекает вектор признаков для каждого пакета. Вектор фиксирует временной контекст канала и отправителя пакета. Наблюдаемые объекты отображаются на видимые нейроны ансамбля автокодеров (KitNET https://github.com/ymirsky/KitNET-py).

Набор данных Kitsune был передан в крупнейший репозиторий реальных и модельных задач машинного обучения с протоколом UCI (*аббр. от англ.* Universal Chess Interface) и стал общедоступным в 2019 г. В нем содержится информация о четырех типах атак: разведка (Recon), человек посередине (MitM), отказ в обслуживании (DoS) и вредоносное ПО для ботнетов (Botnet Malware), например, Mirai – вредоносное программное обеспечение, которое заражает устройства IoT, работающие на процессорах ARC, и превращает их в сеть дистанционно управляемых ботов. Последних также называют «зомби». Этот ботнет часто используется для запуска DDoS-атак.

Данные об атаках были получены из коммерческой IP-системы наблюдения и сети, включающей устройства IoT. Каждый набор данных содержит миллионы сетевых пакетов и различные кибератаки.

Для каждого типа атак имеется следующий набор данных:

– предварительно обработанный набор данных, который готов для применения алгоритмов машинного обучения в формате `.csv`;

– файл с метками (также в формате `.csv`);

– исходный захваченный сетевой трафик в формате `.pcap`.

В таблице 1 представлены типы и виды сетевых атак, которые содержатся в наборе данных Kitsune. В исследовании анализировались фрактальные свойства трафика IoT до и во время воздействия атак: SSDP Flood (длительность 54 сек.), Mirai (44 мин.), OS Scan (длительность 29 сек.), представленные на рисунке 2.

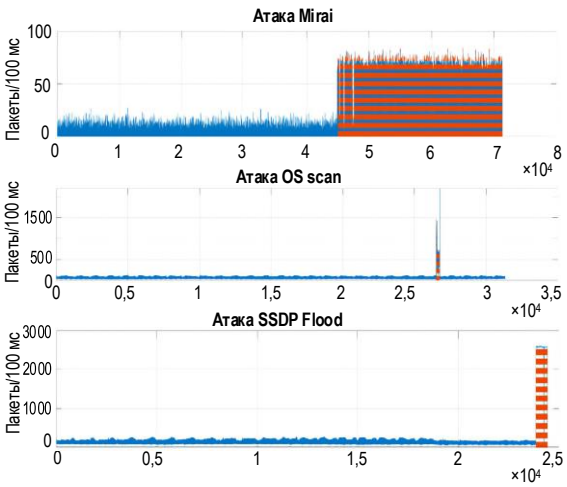


Рис. 2. Трафик IoT: нормальный (голубой); с атакой (красный)

Fig. 2. IoT Traffic: Normal Traffic (Blue), Attack Traffic (Red)

Для оценки фрактальных свойств использовался трафик пакетов, захваченный в скользящем окне с интервалом захвата в 100 мс. В таблице 2 представлены характеристики предварительно обработанного набора данных в формате `.csv`, а также вектор меток, соответствующий исходному сетевому захвату в формате `.pcap`.

Каждая строка csv-файла представляет собой перехваченный и обработанный пакет и содержит информацию о временной статистике, которая

описывает контекст передачи этого пакета, включая данные о хостах и протоколах, участвовавших в передаче. Эта информация содержит 115 различных статистических данных (атрибутов), относящихся к отправителю пакета и трафику между отправителем и получателем. Сбор статистики осуществлялся для всего трафика, который отправляется от источника, используя исходный MAC-адрес и IP-адрес пакета (SrcMAC-IP). Для получения дополнительной информации при анализе трафика использовался и исходный IP-адрес пакета (SrcIP). Для изучения канала связи между исходным и целевым IP-адресами пакета (обозначенного как канал) можно анализировать отправляемые данные. Для изучения сетевых соединений, которые обозначаются как Socket и определяются между источником и получателем пакета, использовалась информация о сокете протокола TCP/UDP.

Общее количество признаков (атрибутов), которые можно извлечь из одного временного окна анализа, составляет 23. Для извлечения атрибутов используется пять окон анализа различной длительности: 100 мс, 500 мс, 1,5 сек., 10 сек. и 1 мин., что в совокупности позволяет создать 115 атрибутов. При отсутствии данных в пакете протокола TCP/UDP соответствующие функции обнуляются.

ТАБЛИЦА 1. Информация об атаках

TABLE 1. Attack Information

Тип атаки	Название атаки	Описание	Вектор атаки	Количество пакетов	Длительность, мин.
Recon	OS Scan	Атакующий сканирует хосты в сети и их операционные системы, пытаясь обнаружить возможные уязвимости	1	1 697 851	52,2
	Fuzzing	Атакующий сканирует на наличие уязвимостей веб-сервер камер посредством отправки случайных команд	3	2 244 139	85,5
Man in the Middle	Video Injection	Злоумышленник встраивает записанное видео в общий видеопоток	1	2 472 401	33,4
	ARP MitM	Злоумышленник перехватывает весь LAN-трафик посредством ARP-атаки	1	2 504 267	28,2
	Active Wiretap	Злоумышленник перехватывает весь сетевой трафик через активную прослушку (сетевой мост), установленную на оголенном кабеле	2	4 554 925	95,6
Denial of Service	SSDP Flood	Злоумышленник перегружает видеорегистратор, заставляя камеры рассылать спам на сервер рекламными объявлениями	1	4 077 266	40,8
	SYN DoS	Злоумышленник отключает видеопоток камеры, перегружая ее веб-сервер	1	2 771 276	52,8
	SSL Renegotiation	Злоумышленник отключает видеопоток камеры, отправляя на нее множество пакетов повторного согласования SSL	1	6 084 492	65,6
Botnet Malware	Mirai	Злоумышленник заражает устройства IoT вредоносным программным обеспечением Mirai, используя учетные данные по умолчанию, а затем сканирует новую уязвимую сеть жертвы	*X*	764 137	118,9

ТАБЛИЦА 2. Характеристики набора данных Kitsune

TABLE 2. Characteristics of the Kitsune Dataset

Тип атаки	Название атаки	Количество пакетов
Вредоносное программное обеспечение для ботнетов	Mirai	764 136
Отказ в обслуживании	SSL Renegotiation	2 207 570
	SSDP Flood	4 077 265
	SYN DoS	2 771 275
Человек посередине	ARP MitM	2 504 266
	Видеоинъекция	2 472 400
	Активная прослушка	2 278 688
Разведка	Сканирование ОС	1 697 850
	Fuzzing	2 244 138

Экспериментальная оценка статистических параметров ФР

Наиболее часто для оценки показателя Херста, характеризующего ФР, используются анализ нормированного размаха (R/S-метод), график изменения дисперсии и вейвлет-анализ [6, 7].

При использовании R/S-метода для заданного набора наблюдений X со средним:

$$\overline{X} = \frac{1}{n}\sum_{j=1}^{n} X_j,$$

где n – количество наблюдений, вводится понятие размаха (разности между максимальным и минимальным отклонением):

$$R(n) = \max\Delta_j - \min\Delta_j,$$

где $1 \le j \le n;\ \Delta_k = \sum_{i=1}^{k}(X_i - k\overline{X}); \forall k = \overline{1,n}$,

$$S(n) = \frac{1}{n}\sum_{j=1}^{n}\left(X_j - \overline{X}\right)^2.$$

Для многих природных явлений математическое ожидание нормированного размаха примерно равно cn^H при $n \to \infty$, где c – положительная константа, не зависящая от n. В результате показатель H можно оценить, изобразив график зависимости $\log(M\frac{R(n)}{S(n)})$ от $\log(n)$, и, используя полученные точки, подобрать по методу наименьших квадратов прямую линию с наклоном H [6, 7].

Чтобы определить количественное значение H, используется соотношение в виде:

$$H = \frac{\ln(R/S)}{\ln(n/2)}. \quad (1)$$

Для оценки ФР в режиме реального времени используется оценка показателя Херста в скользящем окне размера L. Для нейтрализации резких выбросов и уменьшения дисперсии искажений в работе [9] предлагается воспользоваться процедурой трешолдинга (*от англ.* Thresholding) – T. Под трешолдингом понимают метод очистки сигналов от шумов, основанный на вейвлет-преобразовании.

В результате использования трешолдинга формула для текущей оценки показателя Херста [9, 10] приобрела следующий вид:

$$H(t_m) = \sum_{l=1}^{L_0} a_l^{(H)}\phi_l^{(H)}(t_m) + \sum_{j=1}^{J}\sum_{l=1}^{L_j} T\left(d_{j,l}^{(H)}\right)\psi_{j,l}^{(H)}(t_m), \quad (2)$$

где $\phi_l^{(H)}(t_m)$, $\psi_{j,l}^{(H)}(t_m)$ – базисная масштабирующая и вейвлет-функция; $a_{j_0,l}^{(H)}$, $d_{j,l}^{(H)}$ – аппроксимирующие и детализирующие коэффициенты оценки показателя Херста при m-м положении окна фильтрации; $T(d_{j,l}^{(H)})$ – отфильтрованные с помощью преобразования трешолдинга детализирующие вейвлет-коэффициенты; $L_0 = 2^{J_{\max}}$, $(L_0 \le L)$; $J_{\max} = [\log_2 L]$ – максимальное число масштабов разложения; $[\log_2 L]$ – целая часть числа; масштабный коэффициент аппроксимации, равный 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, определяется согласно выражению:

$$a_{j_0,l}^{(H)} = \left\langle \hat{H}(t_m), \phi_l^{(H)} \right\rangle;$$

вейвлет-коэффициент детализации масштаба j, равный скалярному произведению оценки показателя Херста $\hat{H}(t_m)$ и вейвлета масштаба j, смещенного на l единиц масштаба вправо от начала координат, определяется согласно выражению:

$$d_{j,l}^{(H)} = \left\langle \hat{H}(t_m), \psi_{j,l}^{(H)} \right\rangle,$$

Воспользовавшись соотношениями (1) и (2) для обработки экспериментальных данных трафика IoT, были получены статистические характеристики показателя Херста. На рисунке 3 представлены зависимости вычисленных статистических параметров ФР – M_H и D_H – для дампа нормального трафика и под атакой Mirai.

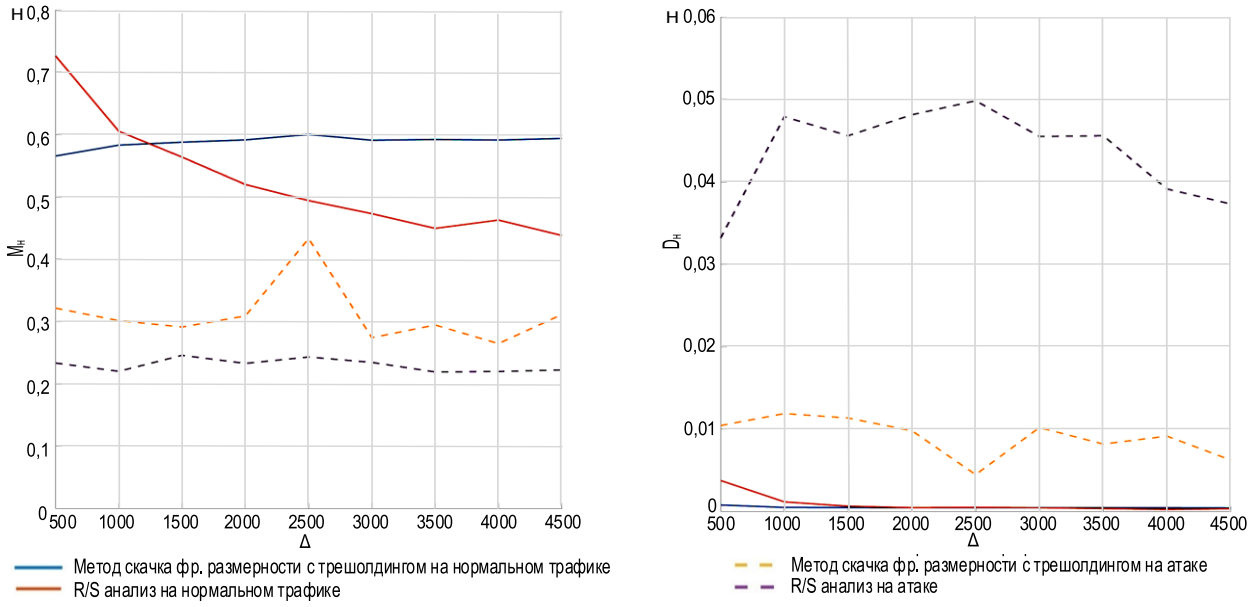


Рис. 3. Зависимости статистических параметров показателя *H* от размера окна анализа Δ для дампа нормального трафика IoT и в условиях воздействия атаки Mirai: M_H – слева; D_H – справа

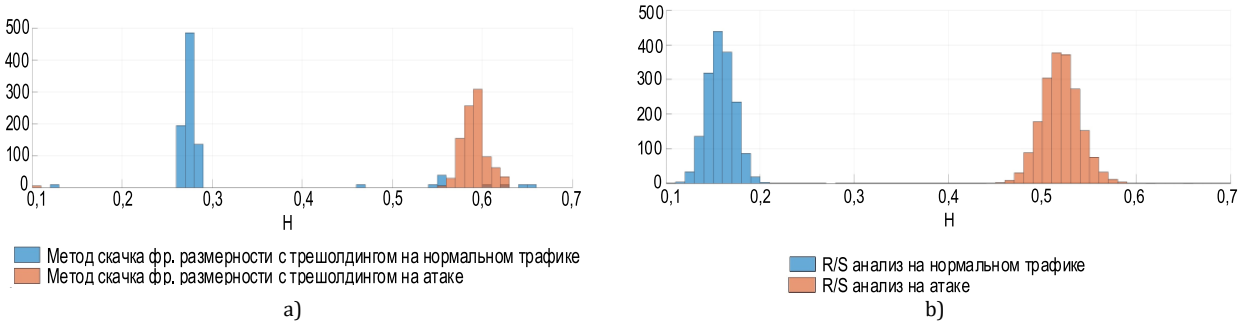
Fig. 3. Dependencies of Statistical Parameters of Indicator H on Analysis Window Size for Normal IoT Traffic Dump and under Mirai Attack: M_H – on the left; b) D_H – on the right

Сравнительный анализ представленных зависимостей показывает, что оценка указанных статистических характеристик с помощью R/S-метода и вейвлет-анализа дает в целом близкие результаты. Разброс в M_H составляет порядка 0.1, а для D_H не превышает 0.03. Различие в оценках объясняется скользящим характером оценок ФР в случае вейвлет-анализа.

Прокомментируем гистограммы распределения оценки показателя Херста на рисунке 4. Качественный анализ полученных результатов показывает, что при воздействии атаки Mirai трафик IoT имеет показатель Херста в интервале $0 < H < 0{,}5$. Это означает, что анализируемый случайный процесс не обладает самоподобием.

В свою очередь, как это видно из рисунков 3 и 4, при отсутствии атак трафик обладает фрактальными свойствами, что может быть положено в основу алгоритма обнаружения атак в сетях. На рисунке 5 показана оценка показателя Херста в скользящем окне при использовании двух рассмотренных выше алгоритмов оценки.

Атака Mirai может быть уверенно обнаружена при превышении текущей оценки показателя Херста и соответствующем выборе порогового уровня $H_{\text{пор}}$ (см. рисунки 5a и 5b). На рисунках 5c и 5d показана текущая оценка показателя Херста в скользящем окне при использовании двух алгоритмов оценки для атаки OS Scan.



a) b)

Рис. 4. Распределение показателя Херста для дампа нормального (голубой) трафика IoT и под атакой Mirai (красный) при Δ = 200 сек. и использовании метода скачка ФР с трешолдингом (a) и *R/S* анализа (b)

Fig. 4. Distribution of the Hurst Exponent for a Normal IoT Traffic Dump and a Mirai Attack at Δ = 200 sec Using the Algorithm: a) Method of Fixing Jumps of the Fractal Dimension with Thresholding; b) R/S Analysis

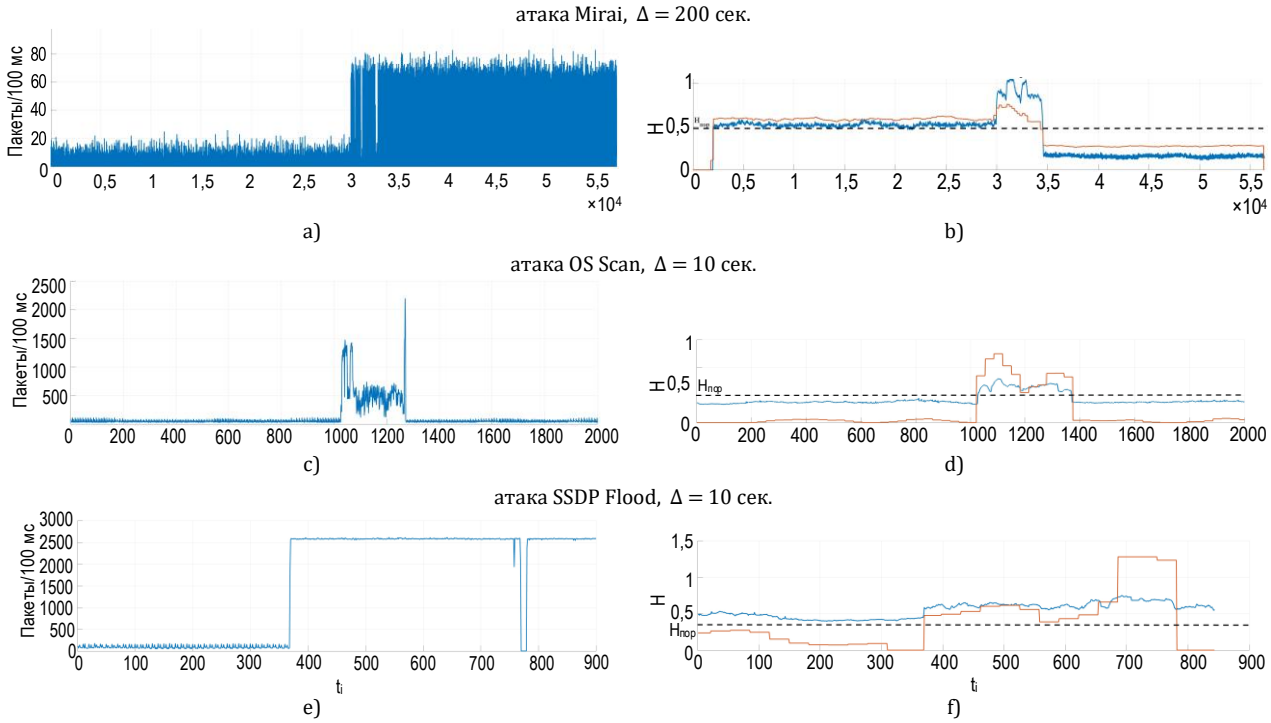


Рис. 5. Оценка *H* трафика IoT при использовании алгоритмов (1) и (2): a), c), e) фрагмент трафика с атакой; b), d), f) – оценка показателя Херста в скользящем окне

Fig. 5. Estimation H of IoT Traffic Using Algorithms (1) and (2): a), c), e) Fragment of Traffic with Attack; b), d), f) – Estimation of the Hurst Exponent in a Sliding Window

Анализ численных значений показателя Херста, представленных на рисунках 5c и 5d, показывает, что трафик IoT в отсутствие атак не обладает фрактальными свойствами, а при появлении атаки OS Scan они наблюдаются, что может быть положено в основу алгоритма обнаружения. Данное явление можно объяснить спецификой трафика устройств IoT. Как и в случае атаки Mirai, атака OS Scan может быть уверенно обнаружена при превышении текущей оценки показателя Херста порогового уровня $H_{пор}$ (см. рисунок 5d). Аналогичные результаты наблюдаются и для атаки SSDP Flood. Численное значение показателя Херста при использовании алгоритмов (1) и (2) представлены на рисунках 5e и 5f.

Сравнительный анализ зависимостей, представленных на рисунке 5, показывает, что лучшие результаты оценки ФР атак показывает алгоритм (2), реализующий метод текущей оценки ФР, основанный на вейвлет-анализе с дополнительной фильтрацией в виде преобразования трешолдинга.

Выводы

По итогам исследования были получены значения статистических параметров фрактальной размерности для нормального трафика в разных точках описанной топологии сети IoT и разных типов атак. Можно сделать вывод о том, что сетевой трафик интернета вещей обладает свойствами самоподобия в том случае, если присутствуют привычные для обычной топологии сети устройства, такие как стационарные ПК и мобильные устройства. Однако в случае, когда компьютерная сеть ограничивается лишь устройствами IoT с низкой пропускной способностью, фрактальные свойства трафика исчезают. В то же время при воздействии атак типа OS Scan и SSDP Flood у анализируемого трафика наблюдаются фрактальные свойства, что может быть использована при создании алгоритмов обнаружения компьютерных атак в сетях IoT. В случае онлайн-анализа сетевого трафика, при оценке ФР следует отдать предпочтение модифицированному алгоритму оценки показателя Херста в скользящем окне анализа (2) с использованием трешолдинга.

Список литературы

1. Minerva R., Biru A., Rotondi D. Towards a definition of the Internet of Things (IoT). Telecom Italia S.p.A., 2015. PP. 10–21. URL: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (Accessed 25.10.2023)

2. Dorsemaine B., Gaulier J.-P., Wary J.-P., Kheir N., Urien P. Internet of Things: A Definition & Taxonomy // Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST, Cambridge, UK, 09–11 September 2015). IEEE, 2015. DOI:10.1109/NGMAST.2015.71

3. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 // Statista. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide (Accessed 12.02.2023)

4. Demeter D., Preuss M., Shmelev Y. IoT: a malware story // Securelist. 2019. URL: https://securelist.com/iot-a-malware-story/94451 (Accessed 11.02.2023)

5. Шевцов В.Ю., Касимовский Н.П. Анализ угроз и уязвимостей концепций IOT и IIOT // НБИ технологии. 2020. Т. 14. № 3. С. 28–35. DOI:10.15688/NBIT.jvolsu.2020.3.5

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

7. Шелухин О.И. Осин А.В. Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. М.: Физматлит. 2008. 368 с.

8. Sheluhin O.I., Lukin I.Yu. Network traffic anomalies detection using fixing method of jumps of multifractal dimension in the real-time mode // Automatic Control and Computer Sciences. 2018. Vol. 52. Iss. 5. PP. 421–430. DOI:10.3103/S01464 11618050115

9. Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме online // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 117–126. DOI:10.31854/1813-324X-2022-8-3-117-126

10. 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 Conference on Wave Electronics and its Application in Information and Telecommunication Systems (WECONF, St. Petersburg, Russia, 30 May – 03 June 2022). IEEE, 2022. DOI:10.1109/WECONF55058.2022. 9803635

11. Sheluhin O.I., Rakovskiy D.I. Multi-Label Learning in Computer Networks // Proceedings of the Conference on Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow, Russia, 14–16 March 2023). IEEE, 2023. DOI:10.1109/IEEECONF56737.2023.10092157

12. Большаков А.С., Губанкова Е.В. Обнаружение аномалий в компьютерных сетях с использованием методов машинного обучения // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10. № 1. С. 37–42.

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

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

15. Alabdulatif A., Rizvi S.S.H. Machine Learning Approach for Improvement in Kitsune NID // Intelligent Automation & Soft Computing. 2022. Vol. 32. Iss. 2. PP. 827–840. DOI:10.32604/iasc.2022.021879

References

1. Minerva R., Biru A., Rotondi D. *Towards a definition of the Internet of Things (IoT).* Telecom Italia S.p.A.; 2015. p.10–21. URL: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf [Accessed 25.10.2023]
2. Dorsemaine B., Gaulier J.-P., Wary J.-P., Kheir N., Urien P. Internet of Things: A Definition & Taxonomy. *Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST, Cambridge, UK, 09–11 September 2015).* IEEE; 2015. DOI:10.1109/NGMAST.2015.71
3. *Statista*. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide [Accessed 12.02.2023]
4. *Securelist*. Demeter D., Preuss M., Shmelev Y. IoT: a malware story. 2019. URL: https://securelist.com/iot-a-malware-story/94451 [Accessed 11.02.2023]
5. Shevtsov V.Y., Kasimovsky N.P Threat and vulnerability analysis of IoT and IIoT concepts. *NBI technologies.* 2020;14(3): 28–35. DOI:10.15688/NBIT.jvolsu.2020.3.5
6. Sheluhin O. I. *Network Anomalies. Detection, Localization, Forecasting.* Moscow: Goryachaya liniya – Telekom Publ.; 2019. 448 p.
7. Sheluhin O.I., Osin A.V., Smolsky S.M. *Self-Similarity and Fractals*. Telecommunication. Moscow: Fizmatlit Publ.; 2008. 368 p.
8. Sheluhin O.I., Lukin I.Yu. Network traffic anomalies detection using fixing method of jumps of multifractal dimension in the real-time mode. *Automatic Control and Computer Sciences.* 2018;52(5):421–430. DOI:10.3103/S0146411618050115
9. Sheluhin O., Rybakov S., Vanyushina A. Modified Algorithm for Detecting Network Attacks Using the Fractal Dimension Jump Estimation Method in Online Mode. *Proceedings of Telecom. Univ*. 2022;8(3):117–126. DOI:10.31854/1813-324X-2022-8-3-117-126
10. 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 Conference on Wave Electronics and its Application in Information and Telecommunication Systems. WECONF, 30 May – 03 June 2022, St. Petersburg, Russia.* IEEE; 2022. DOI:10.1109/WECONF55058.2022.9803635
11. Sheluhin O.I., Rakovskiy D.I. Multi-Label Learning in Computer Networks. *Proceedings of the Conference on Systems of Signals Generating and Processing in the Field of on Board Communications, 14–16 March 2023, Moscow, Russia.* IEEE; 2023. DOI:10.1109/IEEECONF56737.2023.10092157
12. Bolshakov A.S., Gubankova E.V. Anomaly detection in computer networks using machine learning methods. *REDS: Telecommunication Devices and Systems*. 2020;10(1):37–42.
13. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. *arXiv:1802.09089*. 2018. DOI:10.48550/arXiv.1802.09089
14. Miyamoto K., Goto H., Ishibashi R., Han C., Ban T., Takahashi, et al. Malicious Packet Classification Based on Neural Network Using Kitsune Features. *Proceedings of the Second 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
15. Alabdulatif A., Rizvi S.S.H. Machine Learning Approach for Improvement in Kitsune NID. *Intelligent Automation & Soft Computing*. 2022;32(2):827–840. DOI:10.32604/iasc.2022.021879

Статья поступила в редакцию 18.06.2023; одобрена после рецензирования 01.08.2023; принята к публикации 02.11.2023.
The article was submitted 18.06.2023; approved after reviewing 01.08.2023; accepted for publication 02.11.2023.

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 — аспирант кафедры «Информационная безопасность» Московского технического университета связи и информатики
https://orcid.org/0000-0002-4593-9009