МИНОБРНАУКИ РОССИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»
(ФГАОУ ВО «СПбПУ»)

ИНН 7804040077, ОГРН 1027802505279, ОКПО 02068574
ул. Политехническая, д. 29 литера Б,
вн. тер. г. муниципальный округ Академическое,
г. Санкт-Петербург, 195251
тел.:+7(812)552-60-80, office@spbstu.ru

В диссертационный совет 24.2.385.09 при федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна»

ОТЗЫВ

официального оппонента, д.т.н., доцента Павленко Евгения Юрьевича на диссертацию Рыбакова Сергея Юрьевича «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

Актуальность темы исследования

Диссертационная работа Рыбакова С.Ю. посвящена одной из ключевых проблем современной кибербезопасности – обнаружению и классификации компьютерных атак в условиях нестационарности сетевого трафика, высокой вариативности сценариев нарушителя и непрерывного роста доли сегментов Интернета вещей (IoT). В реальных сетях, особенно в промышленном Интернете вещей и киберфизических системах, классические методы анализа трафика и машинного обучения сталкиваются с целым комплексом ограничений – с зависимостью от полноты данных и качества разметки, высокой чувствительностью к «устареванию» данных, трудностями фиксации момента начала атаки и, как следствие, на практике эти методы характеризуются значимой долей ложных срабатываний и пропусков атак.

Фрактальная и мультифрактальная природа сетевого трафика, хорошо известная по работам отечественных и зарубежных авторов, открывает возможность «извлекать» из трафика дополнительные, глубинные признаки, описывающие изменение внутренней структуры потоков под воздействием атак. Использование таких признаков в сочетании с методами машинного

обучения позволяет существенно повысить чувствительность систем обнаружения вторжений, особенно на коротких окнах наблюдения.

В этом контексте выбранная соискателем постановка задачи – построение моделей и алгоритмов обнаружения и классификации атак, базирующихся на комбинации мультифрактального анализа и машинного обучения, – **несомненно, является актуальной** и полностью соответствующей современным тенденциям развития методов защиты информации. Актуальность подтверждается также направленностью работы на сегменты IoT-сетей, где требования к быстродействию, работе на малых окнах и устойчивости к неполной априорной информации особенно жесткие.

Оценка содержания диссертации и автореферата

Диссертация представляет собой завершённое научное исследование, отличающееся внутренней целостностью и логичной структурой. Работа состоит из введения, четырех глав, заключения, списка использованных источников (125 наименований) и шести приложений. Основное содержание изложено на 122 страницах машинописного текста, иллюстрировано 39 рисунками и 19 таблицами, что свидетельствует о существенном объеме проведённых теоретических и экспериментальных исследований.

Во введении обоснованы актуальность темы, степень её разработанности, сформулированы объект и предмет исследования, цель диссертационного исследования и комплекс частных задач. Чётко указана связь диссертационной работы с прикладными задачами обеспечения информационной безопасности в современных компьютерных сетях.

В первой главе выполнен детальный аналитический обзор известных подходов к обнаружению и классификации компьютерных атак методами машинного обучения, а также методами фрактального и мультифрактального анализа, применяемыми к сетевому трафику. На основе сопоставления известных алгоритмов выявлены их ключевые ограничения, такие как зависимость от объема разметки (для методов машинного обучения), недостаточная точность в онлайн-режиме и высокая вариативность качества оценки фрактальных характеристик при работе на коротких окнах (для фрактальных и мультифрактальных методов). Проведенный обзор не носит формального характера, а реально подводит к постановке собственных задач диссертанта.

Во второй главе разработан методический аппарат оценки фрактальных свойств сетевого трафика и компьютерных атак в режиме реального времени на основе дискретного вейвлет-анализа и показателя Херста. Значимым результатом является модифицированная модель оценки

фрактальной размерности, в основе которой лежит вторичная фильтрация детализирующих коэффициентов вейвлет-разложения. Показано, что такая обработка позволяет существенно уменьшить дисперсию текущих оценок показателя Херста, сохранив при этом несмещенность оценки, что критически важно для надежной фиксации малых и кратковременных аномалий в трафике.

Третья глава посвящена постановке и исследованию задач обнаружения компьютерных атак на основе анализа динамики фрактальной размерности. Формализована процедура фиксации скачков фрактальной размерности как задача статистической проверки гипотез о наличии/отсутствии атаки в окне наблюдения, введено пороговое правило по показателю Херста и исследованы зависимости вероятности правильного обнаружения и вероятности ошибки второго рода от порогового уровня и длины окна. Отдельно анализируется влияние числа уровней вейвлет-разложения и параметров трешолдинга на характеристики обнаружения.

В четвёртой главе разработан и исследован метод композиции мультифрактального анализа и алгоритмов машинного обучения для многоклассовой классификации атак. Введено понятие мультифрактального спектра фрактальной размерности (МСФР) трафика, на основе которого формируются новые атрибуты – статистики параметров спектра на различных временных масштабах. Эти признаки интегрируются с традиционными признаками трафика в моделях машинного обучения, что позволяет существенно улучшить качество классификации на реальных и общепринятых наборах данных, в частности, DARPA99, UNSW-NB15, Kitsune для IoT-трафика.

Заключение содержит основные результаты и выводы, полученные в диссертации.

Изложение материала диссертационного исследования является структурированным и логичным, применяемая в работе терминология — корректна. Поставленная в работе цель достигнута.

Автореферат диссертации корректно отражает структуру и основное содержание работы, сформулированные в ней положения, научную новизну, теоретическую и практическую значимость, а также сведения об апробации и публикациях. Материал в автореферате представлен в сжатой, но в целом достаточно информативной форме, логика изложения соответствует структуре диссертации.

Степень обоснованности и достоверность научных положений, выводов и рекомендаций

Обоснованность положений, выносимых диссертантом на защиту, подтверждается применением научного подхода при разработке алгоритмов, их корректным использованием при решении поставленных задач.

Отдельно следует отметить корректность интерпретации результатов. Соискатель явно фиксирует область применимости предложенных моделей и методов, указывает на влияние длины окна наблюдения, параметров трешолдинга, выбора материнского вейвлета и состава признаков на итоговые характеристики обнаружения и классификации.

Достоверность положений, выносимых диссертантом на защиту, подтверждается имитационным моделированием с применением современного математического аппарата, а также внедрением полученных результатов в проектную деятельность ФГУП «НИИ «Квант».

Новизна научных положений, выводов и рекомендаций

Научная новизна полученных автором результатов состоит в следующем:

1. Разработана и математически обоснована модифицированная модель оценки фрактальной размерности сетевого трафика и компьютерных атак в режиме реального времени на основе дискретного вейвлет-анализа с дополнительной фильтрацией детализирующих коэффициентов (трешолдингом), позволяющая существенно снизить дисперсию текущих оценок показателя Херста до 15-40% улучшения точности в зависимости от типа материнского вейвлета без смещения оценки.
2. Предложен новый метод обнаружения и классификации компьютерных атак, отличающийся использованием дополнительной априорной информации о статистических характеристиках фрактальной размерности сетевого трафика и атак. Показано, что использование соответствующих фрактальных признаков позволяет в среднем повысить точность классификации атак примерно на 10% и одновременно сократить время обучения/тестирования ряда алгоритмов машинного обучения.
3. Разработана и реализована модель мультифрактального спектра фрактальной размерности сетевого трафика и атак, учитывающая последовательность текущих оценок фрактальной размерности в окне переменной длины; показано, что параметры МСФР являются информативными признаками для многоклассовой классификации атак.

4. Разработан метод композиции методов машинного обучения и мультифрактального анализа, заключающийся во введении дополнительных атрибутов МСФР в качестве признаков в задаче многоклассовой классификации. Экспериментально показано, что использование таких признаков позволяет повысить качество классификации атак на 7-10% на реальных наборах данных, включая трафик в сетях интернета вещей.

Научные результаты получены автором самостоятельно, что подтверждается наличием публикаций без соавторов, перечисленные результаты диссертационного исследований являются новыми и достоверными.

Теоретическая и практическая значимость результатов работы

Теоретическая значимость состоит в развитии аппарата фрактального и мультифрактального анализа применительно к задачам обнаружения и классификации компьютерных атак в сети. В работе предложены модели оценки фрактальной размерности и мультифрактального спектра, показана возможность их интеграции с методами машинного обучения, уточнены представления о статистических свойствах фрактальных характеристик трафика в присутствии различных типов атак.

Практическая значимость результатов заключается в том, что разработанные методы и алгоритмы обеспечивают повышение достоверности и точности обнаружения атак при работе на коротких окнах наблюдения и в условиях нестационарности сетевого трафика, что критично для современных систем мониторинга. Результаты работы внедрены в проектную деятельность ФГУП «Научно-исследовательский институт «Квант» при проектировании и создании автоматизированных систем в защищенном исполнении и используются в учебном процессе МТУСИ, что подтверждено соответствующими актами внедрения.

Апробация работы и публикации

Основные результаты диссертационного исследования были представлены на 2-х российских и 3-х международных конференциях.

По теме диссертации опубликовано 16 научных работ, в том числе 9 статей в научных изданиях из перечня ВАК РФ, 2 статьи в рецензируемых журналах, индексируемых по базе Scopus, и 4 публикации в материалах конференций и сборниках трудов. Получено свидетельство о государственной регистрации программы для ЭВМ.

Соответствие работы паспорту научной специальности

Диссертация соответствует двум пунктам паспорта специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)»:

– п. 6. «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях»;

– п. 15. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Замечания по диссертации

1. Глубина дискретного вейвлет-разложения, используемого в главе 2 диссертации, выбрана равной шести уровням, при этом критерии отбора уровня масштаба описаны минимально.
2. В работе показана высокая эффективность алгоритма (2.15) для атак типа Mirai и OS Scan. Однако остается неясным, для каких известных типов современных компьютерных атак предложенный метод может оказаться менее эффективным.
3. В главе 4 представлены результаты тестирования модели МСФР, из которых осталось не ясным, как интерпретировать случай, когда расчетное значение показателя Херста превышает единицу. Это формально выходит за рамки классических моделей фрактального анализа и может свидетельствовать о специфическом характере наблюдаемых процессов во время компьютерных атак.
4. Имеют место грамматические ошибки и опечатки в тексте диссертационной работы («подключений для хост» на стр. 25, пропущено слово «числа» в «Снижение ложных срабатываний» на стр. 34, оторванное от основного текста «В связи с изложенным» на стр. 34 и т.п.).

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают ценности представленной диссертационной работы.

Заключение о соответствии диссертации критериям, установленным Положением о присуждении учёных степеней

Диссертационная работа Рыбакова Сергея Юрьевича «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения» по актуальности, научной новизне, теоретической и практической значимости соответствует требованиям, предъявляемым ВАК

Минобрнауки России к диссертациям на соискание учёной степени кандидата технических наук (пп. 9–14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г. (с изменениями и дополнениями)), а также специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)».

Работа является завершённой научно-квалификационной работой, в которой изложены научно обоснованные технические решения и разработки моделей и методов для мониторинга сетевого трафика, обеспечивающие повышение достоверности обнаружения и качества классификации компьютерных атак, имеющие существенное значение для развития страны.

С учётом изложенного, а также принимая во внимание достаточную апробацию результатов и высокий уровень публикационной активности соискателя, считаю, что Рыбаков Сергей Юрьевич заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)».

Официальный оппонент:

доктор технических наук (специальность 2.3.6. «Методы и системы защиты информации, информационная безопасность»), доцент.

доцент Высшей школы кибербезопасности Института компьютерных наук и кибербезопасности ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого».

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Высшая школа кибербезопасности Института компьютерных наук и кибербезопасности.

195251, г. Санкт-Петербург, вн. тер. г. муниципальный округ Академическое, ул. Политехническая, д.29 литера Б

Тел.: +7 (812) 552-76-32

E-mail: pavlenko_eyu@spbstu.ru

Павленко Евгений Юрьевич

«18» ноября 2025 г.