УДК 004.056

ОБНАРУЖЕНИЕ АНОМАЛИЙ В РАБОТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНЫХ ПОКАЗАТЕЛЕЙ

Д.П. Зегжда
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: dmitry@ibks.spbstu.ru

Д.С. Лаврова
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: lavrova@ibks.spbstu.ru

Ключевые слова: обнаружение аномалий, монофрактальный анализ, мультифрактальный анализ, автоматизированные системы управления технологическими процессами

Аннотация: В настоящей статье авторами предложен подход к обнаружению аномалий в работе автоматизированных систем управления технологическими процессами на основе фрактального анализа. В рамках фрактального анализа рассмотрены показатель Херста и характеристики мультифрактального спектра Лежандра – ширина спектра, а также высота и ширина его левой и правой ветвей. Результаты экспериментальных исследований, заключающиеся в моделировании атак на макет автоматизированной системы очистки воды, продемонстрировали состоятельность и эффективность предложенного подхода.

1. Введение

Интеграция интеллектуальных устройств и технологий с различными отраслями деятельности значительно трансформировала всю технологическую инфраструктуру. Автоматизированные системы управления технологическими процессами (АСУ ТП) в большинстве случаев продолжают контролироваться человеком, однако роль человека в них сводится к минимуму.

Интеграция информационных технологий с АСУ ТП и их доступность из сети Интернет делает промышленные системы привлекательным объектом деструктивных кибервоздействий для злоумышленников. Статистика атак за последние несколько лет демонстрирует рост числа кибератак на АСУ ТП, при этом, в большинстве случаев, целью злоумышленников является получение контроля над подсистемой управления. Наиболее критичной является задача сохранения способности АСУ ТП к корректному функционированию даже в условиях деструктивных информационных воздействий, поскольку успешная реализация кибератак на такие системы способна повлечь за собой

негативные финансовые последствия, экологические катастрофы и привести к гибели людей.

Для обеспечения корректного функционирования АСУ ТП в условиях кибератак необходимо своевременно обнаруживать аномалии в работе системы, вызванные попытками злоумышленников реализовать деструктивные кибервоздействия на систему. Подход к обнаружению аномалий должен быть инвариантен к типу кибератак и обеспечивать получение численной характеристики, значение которой будет свидетельствовать о наличии/отсутствии аномалии.

В статье авторами предлагается использовать фрактальный анализ временных рядов, сформированных из значений показателей системы. В качестве численного критерия обнаружения аномалий предлагается использовать отклонение значения коэффициента Херста от нормального для самоподобных (монофрактальных) временных рядов и отклонения значений характеристик мультифрактального спектра Лежандра от нормальных значений для временных рядов, имеющих мультифрактальный характер.

2. Проблема обеспечения информационной безопасности АСУ ТП

Кибератаки представляют собой наиболее эффективный способ воздействия на АСУ ТП, поскольку они позволяют злоумышленникам оказывать скрытное влияние на систему на любом расстоянии. Следует отметить, что целью реализации кибератак на такие системы является не получение информации, а получение контроля над системой, которое позволит не только вывести ее из строя, но и осуществлять гибкое, незаметное изменение параметров ее функционирования, заставляя систему работать нужным образом.

Тенденция к реализации кибератак именно на технологические объекты инфраструктуры стала наблюдаться еще в 2016 году, что подтвердилось ежегодным отчетом с прогнозами по информационной безопасности на 2017 год от компании Trend Micro Incorporated, мирового лидера в разработке решений для кибербезопасности [1]. Наиболее значимой кибератакой 2017 года стала атака на нефтехимический завод в Саудовской Аравии, в рамках которой злоумышленниками была атакована система управления заводом [2]. По данным экспертов, целью атаки было спровоцировать взрыв.

АСУ ТП интегрируются с различными отраслями деятельности человека: производство, энергетика, медицина, транспорт и т.д. Это накладывает особенности на аспекты их функционирования: на количество и состав устройств, на типы и форматы генерируемых ими данных, на используемые протоколы сетевого взаимодействия. Все это затрудняет создание универсального подхода к обнаружению нарушений информационной безопасности АСУ ТП.

Необходимо отметить, что если для компонентов верхнего уровня АСУ ТП используются различные механизмы обеспечения безопасности [3], то компоненты нижнего уровня менее защищены. Значительная часть атак на АСУ ТП реализуется с использованием конечных (полевых) устройств. Ярким примером такой атаки, повлекшей серьезные последствия, является атака с использованием вируса Stuxnet на один из заводов в Иране, в рамках которой были атакованы обогатительные центрифуги завода.

Атаки, направленные на нижние уровни АСУ ТП – уровень датчиков и управляемых механизмов, уровень программируемых контроллеров – приводят к наиболее тяжелым последствиям для системы. При этом, многие атаки реализуются путем подмены данных от конечных устройств, что не всегда легко обнаружить. Необходим подход

к обнаружению аномалий в работе конечных устройств АСУ ТП, обладающий следующими свойствами:

- инвариантностью к типам деструктивных воздействий;
- универсальностью – подход должен быть применим к АСУ ТП любого типа;
- способностью быть интегрированным с АСУ ТП, не требуя настройки или адаптации к обнаружению конкретных видов атак, в том числе, к ранее неизвестным.

Для обнаружения нарушений безопасности в работе АСУ ТП предлагается анализировать данные от конечных устройств, поскольку в них, в соответствии с источником [4], будут отражены информационные управляющие воздействия на систему. Для анализа данных предлагается использовать временные ряды, сформированные из значений показателей конечных устройств. Для обнаружения аномалий используется фрактальный анализ, включающий монофрактальный и мультифрактальный подходы.

3. Обнаружение аномалий с использованием фрактальных показателей

Большинство реальных процессов обладают мультифрактальными свойствами, что подтверждается исследованиями [5-8], а некоторые из них являются монофрактальными. В соответствии с источником [9], мультифрактал – это совокупность фракталов с различной размерностью, определяется несколькими последовательно сменяющимися алгоритмами, каждый из которых генерирует шаблон со своей фрактальной размерностью.

Монофрактальные самоподобные процессы, обладающие одной и той же фрактальной размерностью, также могут быть описаны в рамках мультифрактального формализма. Однако вычисление мультифрактальных характеристик временного ряда представляет собой более сложную задачу, чем проверка наличия у ряда монофрактальных свойств, в связи с этим предлагается сначала проверять временной ряд на свойство монофрактальности, а затем, в случае отсутствия у ряда такого свойства, анализировать его на наличие мультифрактальных свойств.

Показатель Херста H характеризует степень самоподобия процесса. Чем ближе этот параметр к единице, тем более ярко проявляются фрактальные свойства, в соответствии с источником [10]. Напротив, равенство $H = 0{,}5$ говорит об отсутствии самоподобия.

Для описания мультифрактального поведения используется мультифрактальный спектр Лежандра – функция, вычисляемая на основе ряда фрактальных размерностей, входящих в мультифрактал. Мультифрактальный спектр обозначается $f(\alpha)$ и представляет собой меру «частоты» показателя Гельдера $\alpha(t)$ к моменту времени t и показывает вероятность определенного значения показателя. Для вычисления функции мультифрактального спектра необходимо требуется вычислить скейлинговую функцию $\tau(q)$ и осуществить над ней преобразование Лежандра. Вид мультифрактального спектра представлен на рис. 1.

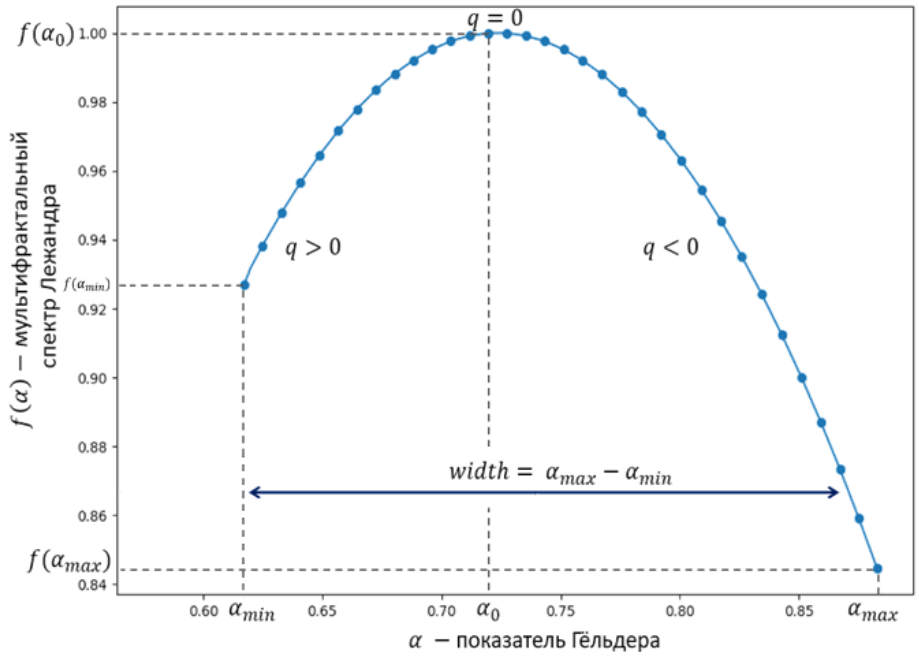

Рис. 1. Мультифрактальный спектр Лежандра.

Контроль значений функции мультифрактального спектра не может быть эффективно использован для обнаружения проблем безопасности в связи с тем, что спектр характеризуется множеством значений функции за определенный промежуток времени. В связи с этим выделены такие характеристики мультифрактального спектра, как ширина и высота, а также ширина и высота его левой и правой ветвей.

При реализации атаки на систему очистки сточных вод был нарушен процесс дехлорирования воды. Атака производилась на расходомер: нарушителем были изменены значения показателя расходомера, в результате чего отключился насос, направляющий дехлорированную воду в блок обратного осмоса. Атака проявилась как аномалия в монофрактальном поведении расходомера и была обнаружена по изменению значения коэффициента Херста (рис. 2): значения коэффициента стали меньше 0,5. Это говорит о нарушении монофрактальности.

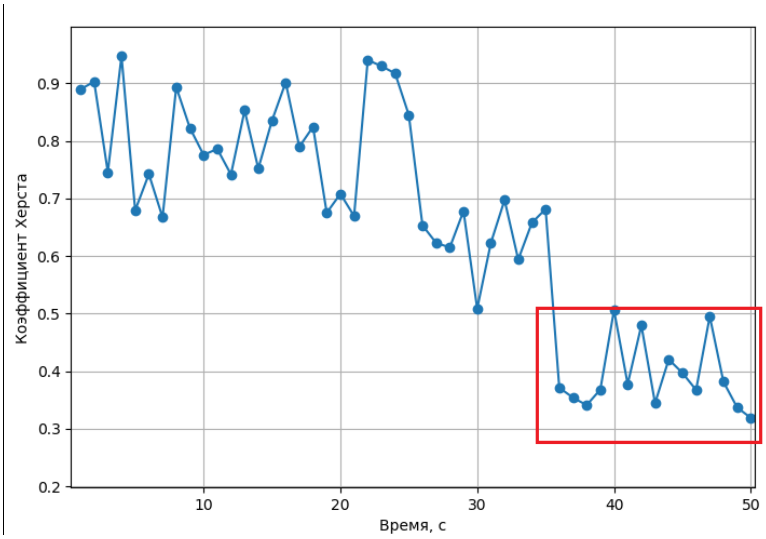

Рис. 2. Обнаружение аномалии с использованием коэффициента Херста.

При реализации атаки на систему очистки сточных вод был нарушен процесс сбора и подготовки поступающих сточных вод. Атака производилась на датчик уровня воды: нарушителем были сфальсифицированы значения датчика, в результате чего переполнился бак, в который поступала вода. Атака проявилась как аномалия в мультифрактальном поведении датчика уровня воды. Аномалия была обнаружена по изменению значения ширины мультифрактального спектра Лежандра, а также по изменению значений ширины левой и правой ветвей спектра (рис. 3).

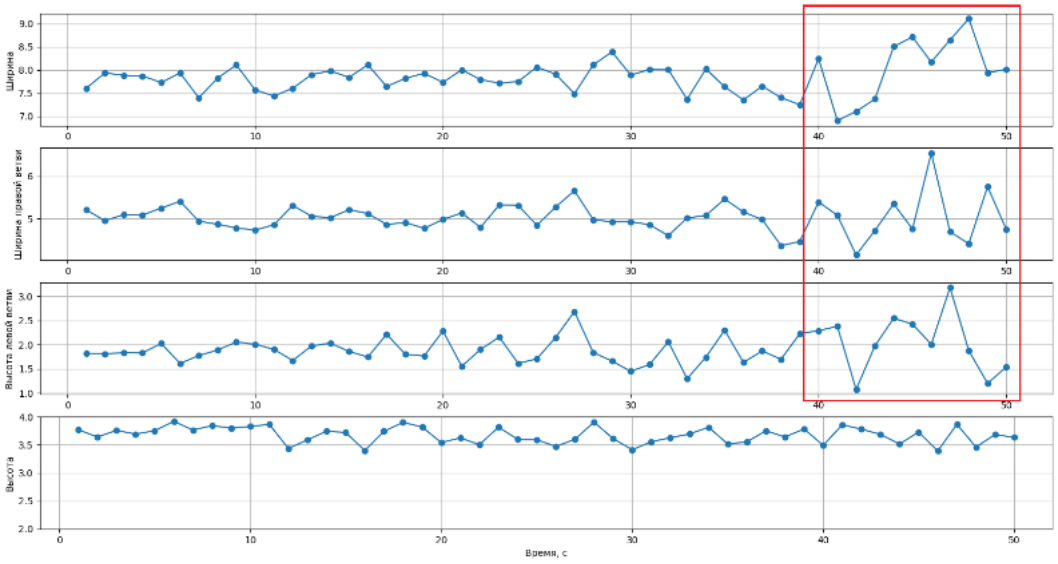

Рис. 3. Обнаружение аномалии с использованием характеристик мультифрактального спектра.

Следует отметить, что различные характеристики мультифрактального спектра Лежандра чувствительны к различным типам атак. В данном случае, можно заметить, что значение высоты спектра менялось одинаково как при нормальной работе системы, так и при реализации атаки.

4. Заключение

Подход к оценке самоподобия параметров функционирования системы с использованием фрактальных показателей продемонстрировал свою эффективность, обнаружив все смоделированные атаки на макет АСУ очистки воды. Предложенный подход универсален за счет представления процессов АСУ ТП в виде временных рядов, инвариантен к типам деструктивных воздействий, и не требует настройки или адаптации к обнаружению конкретных видов атак, в том числе, к ранее неизвестным.

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки ведущих научных школ Российской Федерации НШ-2992.2018.9 (соглашение 075-02-2018-504).

Список литературы

1. The Next Tier - 8 Security Predictions for 2017. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017/.

2. Нефтеперегонный завод чуть не взорвали с помощью трояна. Завод устоял из-за ошибки в коде. http://safe.cnews.ru/news/top/2018-03-21_nefteperegonnyj_zavod_chut_ne_vzorvali_s_pomoshchyu/.
3. Промыслов В. Г., Полетыкин А. Г. Формальная иерархическая модель безопасности верхнего уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. 2012. Т. 4, №. 44. С. 39-53.
4. Лаврова Д.С. Подход к разработке SIEM-системы для Интернета Вещей // Проблемы информационной безопасности. Компьютерные системы. 2016. №2. С. 50-60.
5. Шелухин О. И., Осин А. В. Мультифрактальные свойства трафика реального времени // Электротехнические и информационные комплексы и системы. 2006. Т. 2. №. 3. С. 36-43.
6. Шелухин О. И., Тенякшев А. М., Осин А. В. Фрактальные процессы в телекоммуникациях. М.: Радиотехника, 2003, 480 с.
7. Fisher A., Calvet L., Mandelbrot B. Multifractality of Deutschemark // US dollar exchange rates. 1997. 40 c.
8. Riedi R. H. Multifractal processes. Theory and Applications of Long Range Dependence. Boston: Birkhäuser, 2002, 720 c.
9. Божокин С.В., Паршин Д.А. Фракталы и мультифракталы. Ижевск, 2001. С. 67-70.
10. Треногин Н. Г., Соколов Д. Е. Фрактальные свойства сетевого трафика в клиент-серверной информационной системе // Вестн. НИИ Сибир. гос. ун-та телекоммуникаций и информатики. 2003. № 1. С. 163-172.