ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ МУЛЬТИАГЕНТНЫХ СИСТЕМ УПРАВЛЕНИЯ МИКРОСЕТЯМИ

Гурина Л. А.[1], Томин Н. В.[2]

DOI: 10.21681/2311-3456-2024-6-53-64

Цель исследования: *разработка методов обнаружения и подавления последствий кибератак при вторичном регулировании напряжения в мультиагентных системах управления киберфизическими микросетями.*

Методы исследования: *методы машинного обучения, вероятностные методы*

Результат исследования: *разработаны алгоритм изоляционного леса для автоматического обнаружения кибератак и алгоритм восстановления качества данных на базе метода k-ближайших соседей.*

Научная новизна *состоит в том, что предложенный метод обнаружения кибератак и повышения качества информации создает возможности робастности, адаптации и восстановления мультиагентных систем при нарушениях кибербезопасности.*

Ключевые слова: *киберфизическая микросеть, идентификация кибератак, обнаружение плохих данных, повышение качества информации.*

Введение

Интеллектуальные энергосистемы (ИЭС) возникли с целью повысить гибкость, эффективность, надежность и безопасность энергосетей за счет использования передовых технологий измерения, связи и управления в реальном времени [1, 2]. Преимуществами эксплуатации ИЭС является внедрение информационных, цифровых и коммуникационных технологий, которые позволяют повысить наблюдаемость сети, несмотря на различные неопределенности из-за внутренних и внешних воздействий, тем самым позволяя предпринимать дополнительные корректирующие, превентивные управляющие воздействия. Такая интеграция в ИЭС привела к появлению различных киберфизических взаимозависимостей, что способствует увеличению уязвимостей к киберугрозам на различных уровнях ИЭС: от высоковольтных систем передачи до распределительных сетей и микросетей. Последние в силу активного внедрения объектов распределенной энергетики с привлечением устройств силовой электроники и различных систем управления имеют достаточно сложную информационно-коммуникационную инфраструктуру, отказы и сбои в которой могут оказывать существенно влияние на надежность микросетей.

Концепция микросетей была предложена в качестве организационного принципа управления потоками информации и энергии для сетей с распределенными источниками энергии. В общем смысле микросеть представляет собой объединение источников генерации, нагрузок и систем накопления энергии. С появлением киберфизических микросетей (КФМС) при цифровой трансформации поверхность атак возрастает, что затрудняет обеспечение кибербезопасности (КБ) традиционными методами. Злоумышленники выбирают инновационные методы обхода механизмов безопасности, поэтому существует необходимость разработки и внедрения интеллектуальных методов обеспечения КБ КФМС.

В условиях роста киберугроз традиционные программные системы могут идентифицировать кибератаки (КА) и соответствующим образом модернизировать их, тогда как способность искусственного интеллекта (ИИ) учиться на прошлом опыте может помочь адаптироваться к новым поступающим угрозам. Методы ИИ позволяют не только обнаруживать шаблоны атак в данных и аномалии в них, но и прогнозировать КА. Последовательный анализ шаблонов [3] является одним из методом анализа данных, который позволяет выявить закономерности атак и обнаружить какую-либо вредоносную или аномальную активность.

Одним из основных ограничений использования ИИ в обеспечении КБ является доступность наборов данных. Для обучения модели ИИ используются ретроспективные данные, содержащие сведения о вредоносном программном обеспечении (ПО), шаблонах атак и событиях атак. Используя сигнатуры

1 Гурина Людмила Александровна, кандидат технических наук, доцент, старший научный сотрудник Лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л. А. Мелентьева СО РАН, Иркутск, Россия. E-mail: gurina@isem.irk.ru

2 Томин Никита Викторович, кандидат технических наук, заведующий Лабораторией управления функционированием электроэнергетических систем Института систем энергетики им. Л. А. Мелентьева СО РАН, Иркутск, Россия. E-mail: tomin.nv@gmail.com

событий в наборе данных, ИИ позволяет обнаруживать КА. Недостатком этого метода является сложность создания набора данных. Несмотря на то, что методы ИИ связаны с разработкой интеллектуальных и адаптивных систем, подготовка набора данных на предварительном этапе считается существенным препятствием для использования ИИ в обеспечении КБ. Кроме того, злоумышленники также могут использовать ИИ для обхода механизмов безопасности, поэтому важно знать, как о преимуществах, так и об угрозах, которые представляют собой ИИ в сфере КБ.

Первоначально безопасность ограничивалась атаками на информационные потоки с использованием таких методов, как вредоносное ПО, шпионское ПО и программы-вымогатели. Обеспечение КБ гарантировалось за счет использования антивирусов, межсетевых экранов и систем обнаружения вторжений (IDS). Увеличение числа взаимосвязей и взаимозависимостей между объектами информационно-коммуникационной инфраструктуры КФМС также способствует росту КА. В последнее время алгоритмы машинного обучения стали использоваться для обеспечения КБ различных киберфизических систем [4, 5]. Использование ИИ и, особенно, машинного обучения для обеспечения КБ началось с его внедрения в IDS, что позволяло обнаруживать вредоносное ПО и КА в информационно-коммуникационной инфраструктуре КФМС.

Однако растет обеспокоенность по поводу использования ИИ в сфере КБ. Недавние исследования показали, что системы, КБ которых зависит от алгоритмов машинного обучения, также подвержены различным формам КА. Алгоритмы машинного обучения зависят от данных и, соответственно, делают выводы или прогнозы на основе данных, генерируемых различными датчиками в киберфизических системах. Для формирования успешно реализуемых КА, напр., в КФМС или других объектах ИЭС, требуется разработка методов по манипуляциям с данными, в результате чего могут быть сформированы неправильные управляющие воздействия [6].

Таким образом, использование алгоритмов ИИ и машинного обучения для защиты КФМС также может использоваться злоумышленниками для атаки на них. Такие атаки обладают большим потенциалом, поскольку они более сложны, быстры, трудно обнаруживаемы и подавляемы, поэтому целью данного исследования является разработка метода обнаружения и подавления последствий КА на основе алгоритмов машинного обучения, позволяющих реализовывать стратегии обеспечения КБ КФМС.

Стратегии управления КФМС на основе мультиагентных систем с учетом обеспечения КБ

По аналогии с объектами большой энергетики сегодня для управления микросетями используются три основные стратегии управления в зависимости от их архитектуры: 1) децентрализованные; 2) централизованные и 3) распределенные [7]. Такие архитектуры могут быть представлены и как мультиагентные системы (МАС), когда входные управления могут по-разному зависеть от агентов в зависимости от состояний. С точки зрения МАС такие архитектуры можно математически выразить как:

$$u_i = \begin{cases} u_i(\cup_{j\in v_i} x_i) & \text{(Централизованное)} \\ u_i(x_i \cup_{j\in N_i} x_j) & \text{(Распределенное)} \\ u_i(x_i) & \text{(Децентрализованное)} \end{cases} \quad (1)$$

где u_i – сигнал управления; x_i – состояние i-го агента; v – набор всех агентов.

Согласно (1) сигнал управления u_i может зависеть только от состояния агентов x_i (децентрализованное управление), либо от их x_i и x_j для всех $j \in N_i$ (распределенное управление) (рис. 1). При этом N определяет набор соседних агентов МАС. Цель управления зависит от приложения и многочисленна. Одной из наиболее хорошо изученных задач управления является задача консенсуса, где цель управления агентов состоит в достижении общего состояния, т.е. $\lim_{t\to\infty} |x_i(t) - x_j(t)| = 0 \; \forall_{i,j} \in N_i$.

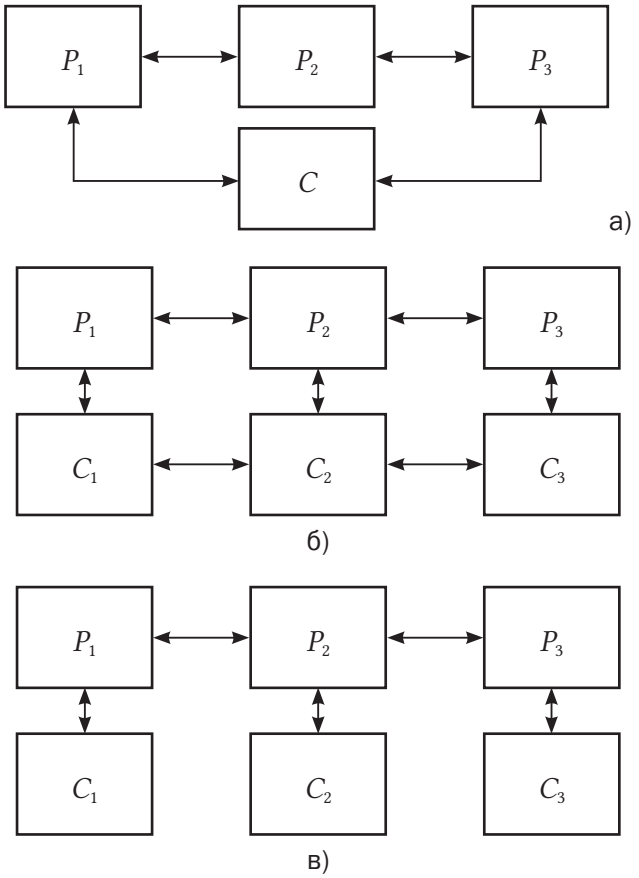


Рис. 1. Иллюстрация (а) децентрализованной, (б) распределенной и (в) децентрализованной архитектур управления. P_1, P_2 и P_3 представляют собой объекты, управляемые контроллерами C_1, C_2 и C_3 соответственно. Адаптировано из [8].

Каждая из стратегий имеет свои преимущества и недостатки. Например, централизованные стратегии способны обеспечить наиболее точное и координированное управление, но при этом обычно требуют полной модели электрической сети, а также имеют проблемы с конфиденциальностью/временем отклика, потери пропускной способности линий связи и единой точки отказа [9]. Децентрализованные и распределенные подходы отчасти лишены подобных проблем, однако связаны с проблемой согласования распределенных управляющих воздействий [10]. Основным принципом таких подходов является обмен информацией между соседними агентами (контроллерами) с использованием распределенного протокола и нахождение консенсуса [11]. На сегодняшний день именно мультиагентные принципы управления КФМС и активными распределительными сетями, включающими объекты распределенной энергетики, рассматриваются как наиболее предпочтительные.

А. Классификация КА на мультиагентные системы управления КФМС

КА на мультиагентные системы управления КФМС можно разделить на атаки на целостность, доступность и конфиденциальность данных (табл. 1) [12]. Наиболее опасными по последствиям КА являются атаки внедрения ложных данных (FDI-атаки), атаки захвата контроллера (Hijacking-атаки), атаки «человек посередине» (MITM-атаки), вредоносное ПО и атаки отказа в обслуживании (DoS-атаки).

Основной целью FDI-атак является изменение значений данных, передаваемых по каналам связи [13]. FDI-атаки увеличивают вычислительную нагрузку на контроллеры, вызывая сбои в управлении устройствами, а также приводят к небалансу мощностей. Злоумышленник нацелен на уязвимости в каналах связи и вводит ложные данные в существующие значения, используя различные методы внедрения [14–16]. Злоумышленник может изменять и удалять данные, что приводит к нарушению целостности и доступности данных.

Вредоносное ПО – это программы, предназначенные для оказания нежелательного или вредоносного воздействия на информационные системы, которые стали серьезной угрозой КБ КФМС. В целом вредоносные программы подразделяются на следующие категории [17]: вирусы, бэкдоры, трояны, черви и шпионское ПО. На практике вредоносное ПО часто демонстрирует характеристики двух или более категорий, например, червь, содержащий полезную нагрузку, может установить черный ход для обеспечения удаленного доступа.

В информационных системах можно нарушить передачу данных в каналах связи между контроллерами с помощью DoS-атак различными способами [18, 19]. Например, можно полностью заблокировать полосу пропускания канала, наводнив его ложной информацией или путем введения буфера в поток коммуникационной связи, что наиболее опасно из-за трудности его идентификации. Последствиями DoS-атак является задержка получения или потеря данных, влекущих за собой нарушение управления КФМС.

Б. Обзор методов машинного обучения, применяемых для обеспечения кибербезопасности КФМС

КА в КФМС не только вызывают проблемы с качеством данных, но и могут привести к сбоям и отказам объектов информационно-коммуникационной инфраструктуры и, как следствие, к нарушениям функционирования самой КФМС. Обмен данными между контроллерами КФМС необходим для достижения эффективного управления ими. Постоянный мониторинг и анализ данных играет важную роль в обеспечении качества данных при КА как на уровне устройства, так и на уровне сети. Важна разработка алгоритмов обнаружения и смягчения/подавления влияния КА на качество данных как на уровне устройства, так и на уровне сети.

Таблица 1.

Классификация кибератак, нарушающих качество данных

Целостность	Доступность	Конфиденциальность
FDI-атака	Jamming-атака	Социальная инженерия
Hijacking-атака	Wormhole-атака	Подслушивание
Подделка данных	DoS-атака	Анализ трафика
Атака повторного воспроизведения	DDos-атака	Несанкционированный доступ
Wormhole-атака	Переполнение буфера	Кража паролей
Spoofing-атака	Puppet-атака	Атака «Человек посередине»,
Атака модификации	Time Synchronization	Атака перехвата
Атака «Человек посередине»	Masquerade-атака	Атака повторного воспроизведения,
Masquerade-атака	Атака «Человек посередине»	Masquerade–атака
	Spoofing-атака	

Первичные и вторичные уровни управления КФМС, несущие важную информацию от контроллеров, наиболее подвержены КА, вызывающим ошибки управления и нарушение функционирование КФМС. Для мониторинга и предотвращения КА на энергетические системы сегодня успешно используются различные алгоритмы машинного обучения. В [20] на основе контролируемых и полуконтролируемых алгоритмов приведена классификация достоверных и искаженных измерений и разработана структура эффективного обнаружения КА. Сильная зависимость от цифровых и коммуникационных технологий увеличивает уязвимости КФМС к атакам внедрения ложных данных, которые могут обойти механизмы обнаружения ошибочных данных. Существующие меры по смягчению последствий FDI-атак либо сосредоточены на избыточных измерениях, либо защищают набор основных измерений. В [21] предложили систему для обнаружения ошибок измерений в результате FDI-атак, основанную на глубоком обучении, для обнаружения аномалий временных рядов используется сверточная нейронная сеть (CNN) и сеть долгосрочной краткосрочной памяти (LSTM). Для оценивания системных переменных учитываются как измерения данных, так и функции сетевого уровня для совместного изучения состояний системы.

Распределенные атаки в отказе обслуживания на контроллеры могут привести к переполнению буфера и потере информации. Авторами [22] предложен алгоритм обнаружения распределенных атак в отказе обслуживания на ранней стадии при помощи шаблона трафика, сгенерированного из набора данных, на основе машины опорных векторов, представляющей собой обученный классификатор. В [23] проанализированы угрозы технологии «интернета вещей». Представлена стратегия обнаружения КА на Интернет вещей, которая объединяет модели генетических алгоритмов и искусственных нейронных сетей. В [24] представлен анализ КА на системы безопасности как на модели IDS, так и на модели беспроводных сенсорных сетей, а также предложены решения по обеспечению безопасности для их устранения на основе модели случайного леса. В [25] для обнаружения вредоносного ПО использована также нейросеть глубокого обучения.

Система прогнозирования КА – это часть системы КБ, которая анализирует данные сетевого трафика в режиме реального времени и прогнозирует КА. Основной мотивацией для прогнозирования КА является повышение точности классификатора в обнаружении КА [26]. Было исследовано и разработано множество подходов к повышению точности прогнозирования КА. Одним из них является машинное обучение [27, 28], которое можно применять как к моделям вторжений, так и к обнаружению КА. Для повышения точности прогнозирования КА в [29] учитывается обнаружения выбросов на основе изоляционного леса с учетом предварительной обработки – несбалансированности набора данных, категориального кодирования признаков и масштабирования признаков.

Метод обнаружения и подавления последствий КА в мультиагентных системах управления КФМС на основе алгоритма изоляционного леса

В [11] была предложена модель мультиагентного контроллера инверторов для распределенного вторичного управления напряжением в электрических сетях и микросетях с высоким уровнем ВИЭ с использованием мультиагентного обучения с подкреплением (англ. Multi-Agent Reinforcement Learning). Такой контроллер реализует управление по статизму $a_{i,t}$, когда амплитуды напряжения V_i инверторов изменяются в зависимости от отклонений реактивной мощности Q_i^m от заданных уставок Q_i^d : $u_i^V = V_i^d - k_{Qi}(Q_i^m - Q_i^d)$, где u_i^V – управляющий сигнал для амплитуды напряжения V_i, V_i^d – желаемая амплитуда напряжения, k_{Qi} – коэффициент усиления по напряжению. Состояние каждого агента i выбирается как $st = (\delta_i, P_i, Q_i, i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}, v_{bdi}, v_{bqi})$ для характеристики режимов распределённых генераторов (РГ), подключенных через инверторы, где δ_i – измеренный опорный угол (фаза); P_i, Q_i – активная и реактивная мощности соответственно; $i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}$ – выходные токи d-q генератора i и напрямую подключенные шины, соответственно; v_{bdi}, v_{bqi} – выходные напряжения d-q подключенной шины соответственно. При этом наблюдение каждого агента включает как свое локальное состояние, так и сообщения от своих соседей: $o_{i,t} = S_{i,t} \cup m_{i,t}$, где $m_{i,t}$ – коммуникационное сообщение, полученное от соседних агентов $j \in N_i$. Целью такого контроллера является максимизация глобального вознаграждения $R_{i,t} = \sum_{k=0}^{T} \gamma^k \sum_{j \in v} \alpha(d_{i,j})\, r_{i,t+k}$, где $\alpha(d_{i,j})\, r_{i,t+k}$ – пространственная функция дисконтирования, $d_{i,j}$ – расстояние между агентом i и j, $r_{i,t}$ – вознаграждение агента i на временном шаге t. При сформулированном вознаграждении $r_{i,t}$ агенты с «аварийными» напряжениями ($V_i \in |0,0.8| \cup |1.25,\infty|$) получат большой штраф, и наоборот агенты с напряжением, близким к 1 о.е. ($V_i \in (|0.95,1.05|)$ получат положительное вознаграждение.

Ранее авторами в [30] была проведена оценка робастности такой концепции вторичного мультиагентного управления к различным типам КА на контроллеры. Испытания показали, что при FDI- и Hijacking-атаках качество регулирования напряжения ухудшается, но не носит критический характер. Во многом это связано с тем, что предложенный

мультиагентный контроллер использует централизованную схему обучения агентов с децентрализованным исполнением, где каждый агент имеет свои собственные актёр-критические нейросети, и их стратегия обновляется независимо с учётом информации от соседних агентов (инверторов) $h_{i,t}$ для повышения скорости сходимости решения и эффективности обучения. Однако это не означает, что такая система регулирования абсолютна робастна к КА, в этом случает требуется встроенная интеллектуальная процедура обнаружения и подавления последствий КА.

В настоящей работе предложена двухэтапная процедура обнаружения и подавления последствий КА с использованием следующих методов машинного обучения без учителя: изоляционный лес (англ. Isolation Forest) и k-ближайших соседей (англ. k-nearest neighbors algorithm, k-NN). Структура ее адаптации в вышеописанную структуру мультиагентного вторичного управления напряжением в КФМС показана на рис. 2 и более подробно раскрыта далее.

А. Алгоритм изоляционного леса для автоматического обнаружения КА

Изоляционный лес – это алгоритм машинного обучения для обнаружения аномалий данных с помощью двоичных деревьев [31]. Алгоритм для обнаружения аномалий опирается на характеристики аномалий, т.е. на то, что их мало и они различны. Суть алгоритма заключается в том, что аномальные точки данных легче отделить от остальной части выборки. Чтобы изолировать точку данных, алгоритм рекурсивно генерирует фрагменты выборки, случайным образом выбирая атрибут, а затем случайным образом выбирая значение разделения между минимальным и максимальным значениями, разрешенными для этого атрибута. Обнаружение аномалий с помощью изоляционного леса – это процесс, состоящий из двух основных этапов:

1) на первом этапе для построения двоичных деревьев используется набор обучающих данных;
2) на втором – каждый экземпляр в тестовом наборе проходит через эти деревья, и экземпляру присваивается надлежащая «оценка аномалии».

После того как всем экземплярам в тестовом наборе присвоен показатель аномалии, можно пометить как «аномалию» любую точку, показатель которой превышает заранее определенный порог, который зависит от области, к которой применяется анализ.

Алгоритм расчета оценки аномалии точки данных основан на наблюдении, что структура дерева эквивалентна структуре двоичных деревьев поиска (англ. Binary Search Trees, BST): завершение внешнего узла дерева соответствует неудачному поиску в BST. Как следствие, оценка среднего $h(x)$ для завершения внешнего узла то же, что и для неудачных поисков в BST, то есть

$$c(m) = \begin{cases} 2H(m-1) - \dfrac{2(m-1)}{n} & \text{для } m > 2 \\ 1 & \text{для } m = 2 \\ 0 & \text{в противном случае} \end{cases} \qquad (2)$$

где n – размер тестовых данных, m – размер выборки и H – номер гармоники, который можно оценить по формуле $H(i) = ln(i) - \gamma$, где γ = 0,5772156649 – постоянная Эйлера-Машерони.

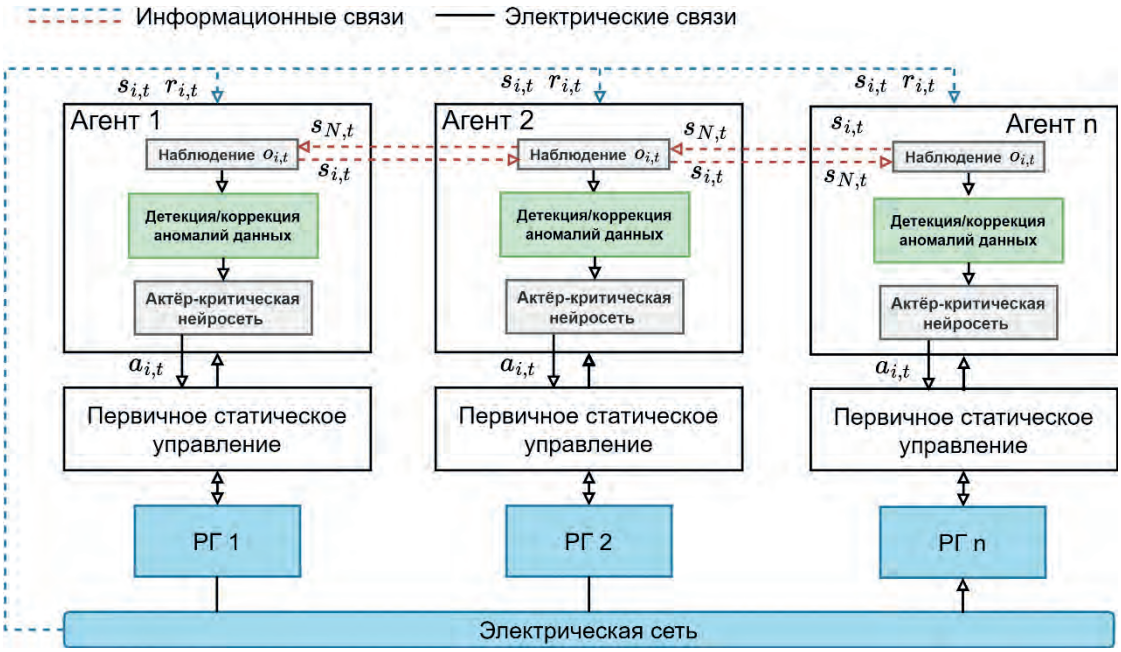


Рис. 2. Общая структура мультиагентного вторичного управления контроллерами инверторов РГ на базе MARL с функцией защиты от КА на основе двухэтапной процедуры

Значение $c(m)$ в (2) представляет собой среднее значение $h(x)$ данный m, поэтому мы можем использовать его для нормализации x и получить оценку оценки аномалии для данного экземпляра x:

$$s(x,m) = 2^{\frac{-E(h(x))}{c(m)}}, \quad (3)$$

где $E(h(x))$ – среднее значение $h(x)$ из коллекции деревьев. Интересно отметить, что для любого данного случая

- если s близко к 1, то x наиболее вероятно является аномалией (рис. 3);
- если s меньше, чем 0.5, то x наиболее вероятно нормальное значение;
- если для данной выборки всем экземплярам присвоен показатель аномалии около 0.5, то можно с уверенностью предположить, что в выборке нет аномалий.

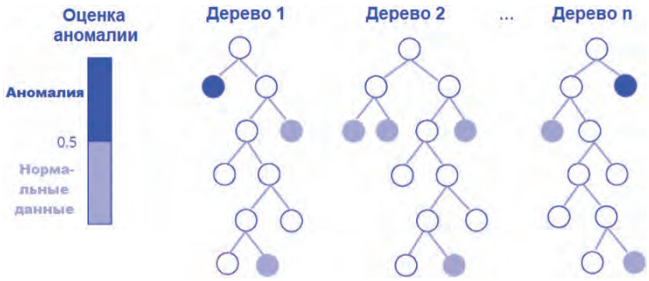


Рис. 3. Общая схема работы метода изоляционного леса

В предлагаемой процедуре в качестве x выступают наблюдения агента $o_{i,t} = S_{i,t} \cup m_{i,t}$, когда потенциальная кибератака может вызывать аномалии как в локальных входных данных агента $S_{i,t}$, так и в сигналах, которые приходят от соседних агентов $m_{i,t}$. В процессе обучения агентов по методу MARL параллельно обучается модель изоляционного леса на данных $o_{i,t}$, которые приходят к агентам. В итоге каждому набору $o_{i,t}$ присваивается значение $S(o_{i,t},m)$, представляющее собой оценку аномалии.

Однако при обнаружении аномалии в каком-либо наборе $o_{i,t}$ мы не можем его просто исключить, так как это фактически означает исключение контроллера из процесса регулирования напряжения. В этом случае помимо обнаружения аномалий (первый этап предложенной процедуры) требуется решение задачи восстановления качества данных в искаженном наборе $o_{i,t}$. Поэтому на втором этапе процедуры предложено применение метода k-ближайших соседей для повышения качества данных.

Б. Алгоритм восстановления качества данных на базе метода k-ближайших соседей

Метод k-ближайших соседей (KNN) для заполнения пропущенных значений в данных основан на предположении, что значения в неиспорченных ячейках зависят от значений в их окрестности [32]. Для каждой ячейки с пропущенным значением x_{ij} во входной матрице данных X размером $n \times m$, где n – количество наблюдений, а m – количество признаков, метод выполняет следующие шаги:

1. Определение окрестности: находятся k ближайших наблюдений к x_{ij} среди всех оставшихся наблюдений, где k – заданное число. Расстояние между наблюдениями обычно измеряется с помощью метрики Минковского: $d(x_i,x_j) = (\sum_{k=1}^{m} (x_{ik} - x_{jk})^p)^{1/p}$. Норма Минковского принимает форму евклидова расстояния или расстояния L2, когда $p = 2$, или форму расстояния Манхэттена, когда $p = 1$; были описаны другие дробные нормы для $p < 1$ [33]. В экспериментах данного исследования было принято $p = 2$.

2. Заполнение пропусков: значение пропущенной ячейки x_{ij} оценивается как среднее арифметическое значений k ближайших соседей: $\hat{x}_{ij} = \frac{1}{K} \sum k \in N(i,k)\ x_{kj}$, где $N(i,k)$ — множество индексов k ближайших соседей к наблюдению i.

Метод KNN для заполнения пропущенных значений может быть использован как для числовых, так и для категориальных данных с небольшими модификациями в подходе к определению близости и способу заполнения пропусков. В данном случае под x_{ij} понимаются «повреждённые» значения вектора наблюдения агента $o_{i,t} = S_{i,t} \cup m_{i,t}$. Так, после КА могут возникнуть аномалии в каких-либо значения вектора локального состояния агента $s_t = (\delta_i, P_i, Q_i, i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}, v_{bdi}, v_{bqi})$ (напр., в $i_{odi}, i_{oqi}, i_{bdi}$) и тогда их восстановление будет зависит от «нормальных» значений других параметров вектора, лежащих в окрестности.

Таким образом, предложенная двухэтапная процедура обнаружения КА и повышения качества данных может быть проиллюстрирована общей блок-схемой, представленной на рис. 4.

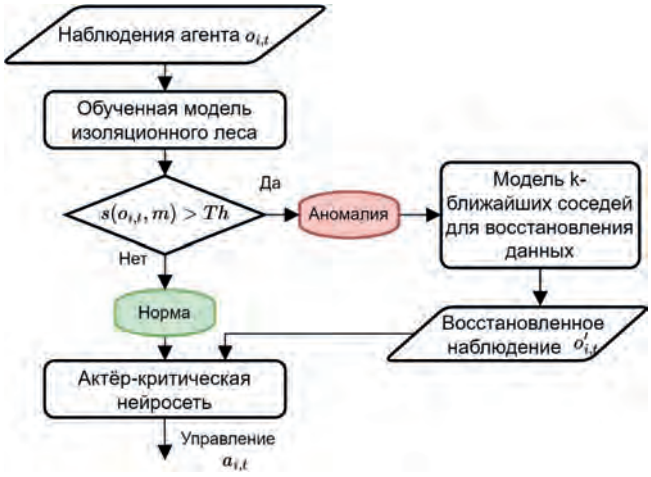


Рис. 4. Общая блок-схема предложенной двухэтапной процедуры обнаружения КА и повышения качества данных с использованием алгоритмов машинного обучения без учителя

Пример

Для оценки эффективности предложенной двухэтапной процедуры обнаружения КА и повышения качества данных, рассмотрим модели сообщества КФМС с шестью распределенными генераторами (РГ) (солнечные фотоэлектрические преобразователи), подключаемыми через AC/DC инверторы к сети переменного тока (рис. 5). При этом КФМС подключены к внешней электрической сети и имеют единую мультиагентную систему вторичного регулирования напряжения, показанную на рис. 2. По аналогии с [30] были рассмотрены несколько сценариев, когда контроллеры инверторов 3, 5 и 6 (агенты) подвергаются воздействию следующих вредоносных воздействий: FDI- и Hijacking-атаки. Для реализации методов изоляционного леса и k-ближайших соседей была использована Python-библиотека Scikit-learn для машинного обучения [34]. Для реализации MARL и модели микросетей были задействованы Python-библиотеки PyTorch и Powernet [35].

Помимо КА, для демонстрации эффективности предложенного варианта вторичного регулирования были смоделированы случайные колебания нагрузки, которые приводят к падению напряжения. Для этого были добавлены случайные изменения нагрузки по всей сети с отклонениями ± 20% от номинальных значений, а также случайные возмущения в диапазоне ±5% для каждой нагрузки схемы, показанной на рис. 5. При этом все агенты в схеме микросетей контролировались со временем выборки 0,05 с, и каждый агент мог связываться со своими соседями через локальные граничные каналы связи. Первичное управление нижнего уровня реализовано по аналогии с [36]. Глобальной целью управления является регулирование всех напряжений РГ до опорного значения 1 о.е.

На рис. 6 показаны оценки аномалий на базе метода изоляционного леса для каждой точки данных в наборе данных при сценарии Hijacking-атаки. Эти оценки соответствуют вектору наблюдения агента $o_{i,t}$, т.е. входному вектору контроллера инвертора. Цвет каждой точки представляет ее оценку аномалии: более темные цвета указывают на более высокие оценки аномальности, а более светлые цвета указывают на более низкие оценки. Таким образом, точки самых темных цветов представляют собой наиболее аномальные точки данных, поскольку они наиболее изолированы от остальных данных. С другой стороны, точки самых светлых цветов являются наименее аномальными точками данных, поскольку они наиболее близки к остальным данным. Хорошо видно, что алгоритм изоляционного леса точно обнаруживает потенциальные аномалии в наблюдениях $o_{i,t}$ подверженных КА агентов 3, 5 и 6 (рис. 6б).

На рис. 7 и 8 представлены результаты моделирования системы регулирования напряжения при возмущении нагрузки для различных сценарных экспериментов FDI- и Hijacking-атаках. В отсутствие КА агенты мультиагентной системы управления хорошо справляются с задачей вторичного регулирования напряжения при случайных колебаниях нагрузки, приводящих к падению напряжения. Фактически с момента времени $t = 0.4\ c.$ агенты формируют кооперативную стратегию, которая успешно восстанавливает и поддерживает все регулируемые напряжения близко к номинальному значению 1 отн.ед. (рис. 7а и 8а).

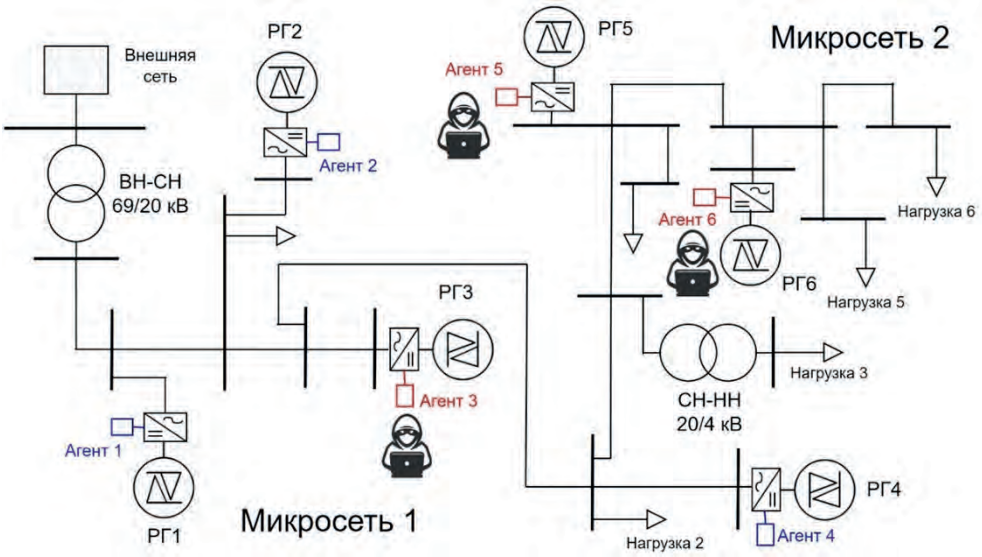
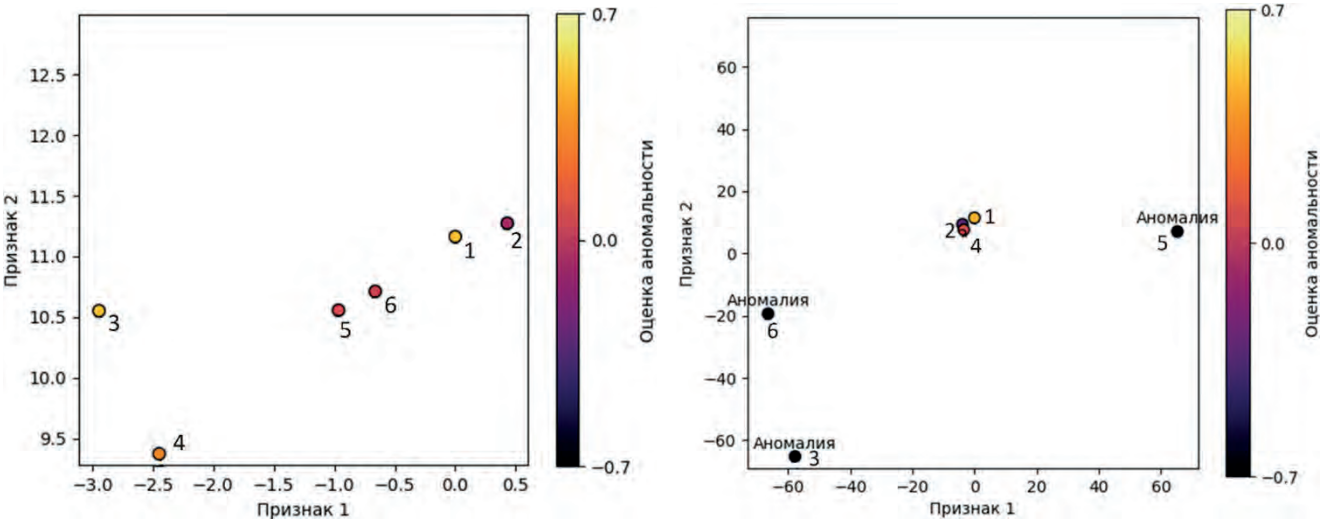
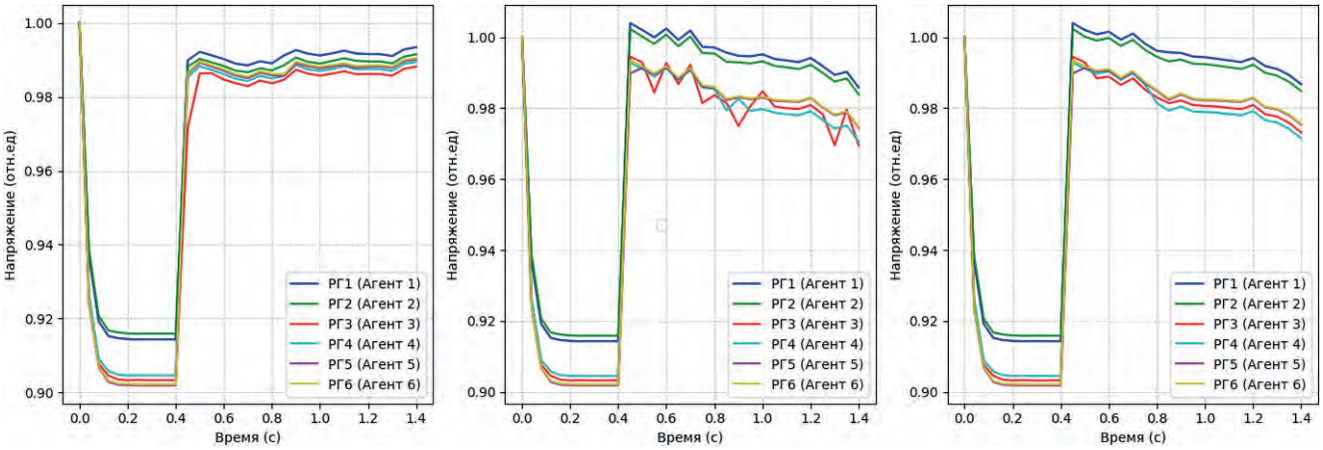


Рис. 5. Тестовая схема двух взаимосвязанных микросетей, имеющих общую систему мультиагентного вторичного регулирования напряжения



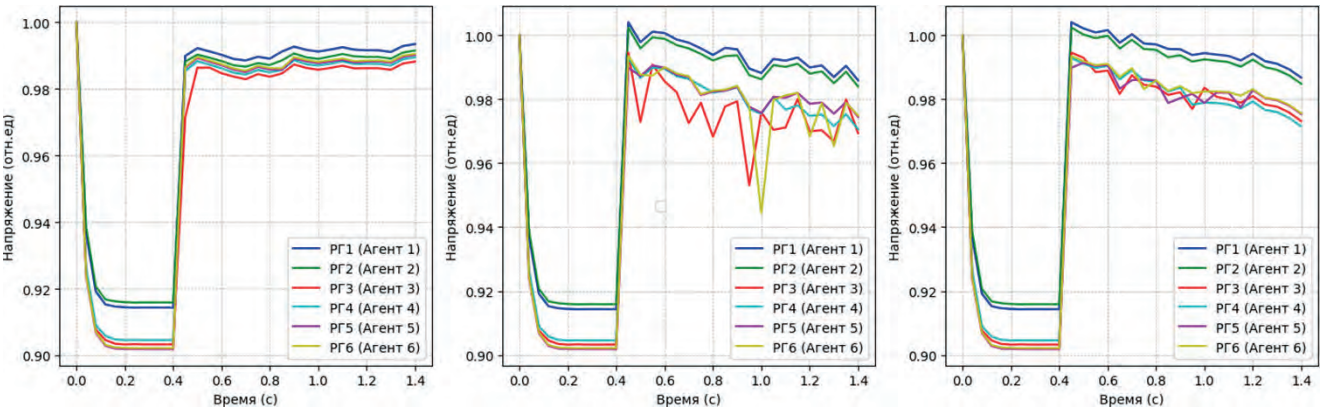
а) В отсутствие КА *б) Hijacking-атака*

Рис. 6. Визуализация оценки векторов наблюдений агентов (контроллеров) на предмет аномальных данных с использованием изоляционного леса



а) В отсутствие КА *б) FDI-атака* *в) Подавление последствий КА*

Рис. 7. Результаты моделирования поведения агентов системы регулирования напряжения при возмущении нагрузки для различных сценарных экспериментов FDI-атаки



а) В отсутствие КА *б) Hijacking-атака* *в) Подавление последствий КА*

Рис. 8. Результаты моделирования поведения агентов системы регулирования напряжения при возмущении нагрузки для различных сценарных экспериментов атаки захвата контроллеров 3, 5, 6.

Таблица 2.

Пример наблюдения $o_{i,t}$ агента-контроллера №3 для различных сценариев КА

№	Сценарий	Вектор наблюдения агента $o_{i,t}$								
		δ_i	P_i	Q_i	i_{odi}	i_{oqi}	i_{bdi}	i_{bqi}	v_{bdi}	v_{bqi}
1	Без кибератаки	–2.53	9.18	10.03	4.19	–5.38	–3.42	3.36	–3.45	3.35
2	Hijacking-атака	–13.6	–7.44	–119	–175	–47.2	–47.1	21.4	–68.1	–75.1
3	Восстановление данных	–0.17	9.58	7.02	5.02	–3.39	–3.41	3.35	–3.45	3.36

При различных вариантах FDI- и Hijacking-атаках на 3, 5 и 6 контроллеры качество вторичного регулирования ожидаемо ухудшается (рис. 7б и 8б). Это выражается в появлении колебаний при регулировании и снижении эффективности общего поддержания уровней напряжения близких к номинальным. Особенно явно это проявляется при сценарии Hijacking-атаке, которая в рассмотренном примере соответствует полному захвату контроллеров, т.е. в $o^*_{i,t} = (1 - \alpha)\, o_{i,t} - \alpha x^{\alpha}_{i,t}$ (где $o^*_{i,t}$ – модифицированное наблюдение агента; $x^{\alpha}_{i,t}$ – ложные данные), коэффициент $\alpha = 1$, что означает атаку на инвертор с полной заменой корректных наблюдений. Возникновение колебаний связано с ухудшением согласованности агентов, т.е. установления консенсуса, в следствии того, что от некоторых агентов поступает ложные данные.

Применение предложенной двухэтапной процедуры, в частности метода k-ближайших соседей, позволяет повысить качество данных подверженным КА контроллеров с определенным значением точности. Восстановление качества данных происходит до того, как будет выработано управляющее воздействие $a_{i,t}$, т.е. согласно рис. 2, перед подачей наблюдения $o_{i,t}$ в актёр-критическую нейросеть конкретного агента. В частности, восстановление качества данных в искаженных наборах $o^*_{i,t}$ приводит к нивелированию несогласованности в мультиагентной системы, и как следствие, уменьшению колебаний (рис. 7в и 8в).

В табл. 2 показан пример одного из наблюдений $o_{i,t}$ атакованного агента-контроллера №3 для различных сценариев для определенного момента времени моделирования t. Хорошо видно, что при Hijacking-атаке наблюдение агента по всем параметрам грубо нарушено и не соответствует действительности, т.е. наблюдается полный захват этого контроллера. Однако применение метода k-ближайших соседей в рамках предложенной процедуры позволяет восстановить качество данных до значений в требуемых пределах.

Выводы

Рассмотрена мультиагентная система управления КФМС. Проведен аналитический обзор методов искусственного интеллекта и машинного обучения для обеспечения КБ КФМС при интеллектуальном управлении ими. Разработан интеллектуальный подход к обнаружению КА и повышению качества данных при вторичном мультиагентном управлении КФМС на основе алгоритмов машинного обучения. Эффективность применения предложенного подхода подтверждена численными расчетами на примере моделирования КА на взаимосвязанные КФМС, имеющих общую систему мультиагентного вторичного регулирования напряжения.

Работа выполнена в рамках научного проекта «Теоретические основы, модели и методы управления развитием и функционированием интеллектуальных электроэнергетических систем», № FWEU-2021-0001.

Литература

1. *N. Voropai. Electric Power System Transformations: A Review of Main Prospects and Challenges // Energies, 2020, vol. 13(21), 5639. DOI:10.3390/en13215639*
2. *Илюшин П. В. Системный подход к развитию и внедрению распределенной энергетики и возобновляемых источников энергии в России // Энергетик, 2022, 4, с. 20–27.*
3. *Nisha T. N., Pramod D. Sequential pattern analysis for event-based intrusion detection // International Journal of Information and Computer Security, 2019, 11(4/5), 476. DOI:10.1504/ijics.2019.101936*
4. *C. Li, M. Qiu. Reinforcement Learning for Cyber-Physical Systems: with Cybersecurity Case Studies. Chapman and Hall/CRC, 2019.*
5. *S. Gaba et al. A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems // IEEE Access, 2024, vol. 12, pp. 6017–6035. DOI: 10.1109/ACCESS.2023.3349022*

6. *F. O. Olowononi, D. B. Rawat and C. Liu. Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS // in IEEE Communications Surveys & Tutorials, Firstquarter 2021, vol. 23, no. 1, pp. 524–552. DOI: 10.1109/COMST.2020.3036778*
7. *Илюшин П. В., Вольный В. С. Обзор структур микросетей низкого напряжения с распределенными источниками энергии // Релейная защита и автоматизация. 2023, № 1(50), с. 68–80.*
8. *Mahela O. P., Khosravy M., Gupta N., et al. Comprehensive Overview of Multi-agent Systems for Controlling Smart Grids // CSEE Journal of Power and Energy Systems, 2022, Vol. 8, No. 1, pp. 115–131. DOI: 10.17775/CSEEJPES.2020.03390*
9. *Jabbar M. A. M., Tran D. T., Kim K. -H. Decentralized Power Flow Control Strategy Using Transition Operations of DC-Bus Voltage for Detection of Uncertain DC Microgrid Operations // Sustainability, 2023, Vol. 15, 11635. DOI: 10.3390/su151511635*
10. *Takayama S., Ishigame A. Volt–Var curve determination method of smart inverters by multi-agent deep reinforcement learning // International Journal of Electrical Power & Energy Systems, 2024, Vol. 157, 109888. DOI: 10.1016/j.ijepes.2024.109888*
11. *Tomin N., Voropai N., Kurbatsky V., Rehtanz C. Management of Voltage Flexibility from Inverter-Based Distributed Generation Using Multi-Agent Reinforcement Learning // Energies, 2021, 14(24), 8270. DOI: 10.3390/en14248270*
12. *Гурина Л. А. Оценка рисков кибербезопасности энергетического сообщества микросетей // Вопросы кибербезопасности. 2024. 1(59). С. 101–107. DOI: 10.21681/2311-3456-2024-1-101-107*
13. *H. Zhang, D. Yue, C. Dou and G. P. Hancke/ Resilient Optimal Defensive Strategy of Micro-Grids System via Distributed Deep Reinforcement Learning Approach Against FDI Attack // in IEEE Transactions on Neural Networks and Learning Systems, Jan. 2024, vol. 35, no. 1, pp. 598–608. DOI: 10.1109/TNNLS.2022.3175917*
14. *I. Tasevski and K. Jakimoski. Overview of SQL Injection Defense Mechanisms // 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2020, pp. 1–4. DOI: 10.1109/TELFOR51502.2020.9306676*
15. *B. Abazi and E. Hajrizi. Practical analysis on the algorithm of the Cross-Site Scripting Attacks // 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP), Sofia, Bulgaria, 2022, pp. 1–4. DOI: 10.1109/IWSSIP55020.2022.9854491*
16. *Mode, G. R.; Calyam, P.; Hoque, K. A. False data injection attacks in internet of things and deep learning enabled predictive analytics. arXiv 2019, arXiv:1910.01716.*
17. *Y. Gao, H. Hasegawa, Y. Yamaguchi and H. Shimada. Malware Detection by Control-Flow Graph Level Representation Learning With Graph Isomorphism Network // in IEEE Access, 2022, vol. 10, pp. 111830–11841. DOI: 10.1109/ACCESS.2022.3215267*
18. *T. Li, B. Chen, L. Yu and W. -A. Zhang. Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems // in IEEE Transactions on Automatic Control, Sept. 2021, vol. 66, no. 9, pp. 4303–4310. DOI: 10.1109/TAC.2020.3032598*
19. *X. Xie, Y. Liu and B. Xu, Resilient event-triggered control for cyber-physical systems under stochastic-sampling and denial-of-service attacks // 2021 40th Chinese Control Conference (CCC), Shanghai, China, 2021, pp. 4702-4708. DOI: 10.23919/CCC52363.2021.9549917*
20. *A. Talati, V. Garg, N. Mishra, P. Tiwari and P. Jena. Cyber-Attack Detection in Smart Grids Using Machine Learning Approach // 2023 7th International Conference on Computer Applications in Electrical Engineering-Recent Advances (CERA), Roorkee, India, 2023, pp. 1–6. DOI: 10.1109/CERA59325.2023.10455586*
21. *X. Niu, J. Li, J. Sun and K. Tomsovic. Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning // 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2019, pp. 1–6. DOI: 10.1109/ISGT.2019.8791598*
22. *S. Pusarla, U. Ghugar, T. Özseven, B. K. Dewangan, T. Choudhury and J. C. Patni. A Compressive Study on Detection Accuracy Model for DoS Attack in SDN Using Ensemble Learning Techniques // 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), Istanbul, Turkiye, 2023, pp. 1-6. DOI: 10.1109/ISAS60782.2023.10391345*
23. *A. Srivastava, H. S. Sharma, R. Rawat and N. Garg. Detection of Cyber Attack in IoT Based Model Using ANN Model with Genetic Algorithm // 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 1198-1201. DOI: 10.1109/IC2PCT60090.2024.10486578*
24. *A. AlBusaidi and F. H. Mohideen. Analysis of Wireless Sensor Network Security Models: A Salient Approach for Deeper Inspection Using Deep Neural Networks // 2023 International Conference on Emerging Techniques in Computational Intelligence (ICETCI), Hyderabad, India, 2023, pp. 276–282. DOI: 10.1109/ICETCI58599.2023.10330927*
25. *S. Puneeth, S. Lal, M. Pratap Singh and B. S. Raghavendra. RMDNet-Deep Learning Paradigms for Effective Malware Detection and Classification // in IEEE Access, 2024, vol. 12, pp. 82622–82635, 2024. DOI: 10.1109/ACCESS.2024.3403458*
26. *P. S. Patil, S. L. Deshpande, G. S. Hukkeri, R. H. Goudar and P. Siddarkar. Prediction of DDoS Flooding Attack using Machine Learning Models // 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1–6. DOI: 10.1109/ICSTCEE56972.2022.10100083*
27. *S. Bala and S. M. M. Ahsan. Detecting DDoS attacks in Software Define Networking: A Machine Learning Based Approach // 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM), Gazipur, Bangladesh, 2023, pp. 1–6. DOI: 10.1109/NCIM59001.2023.10212569*
28. *Sarker I. H. Machine Learning: Algorithms, Real-World Applications and Research Directions // SN Computer Science, 2021, 2(3). DOI:10.1007/s42979-021-00592-x*
29. *Ripan Rony, Md. Moinul Islam, Alqahtani Hamed, Sarker Iqbal H. Effectively predicting cyber-attacks through isolation forest learning-based outlier detection // Security and Privacy, 2022, 5(3). DOI:10.1002/spy2.212*
30. *Гурина Л. А., Томин Н. В. Разработка комплексного подхода к обеспечению кибербезопасности взаимосвязанных информационных систем при интеллектуальном управлении сообществом микросетей // Вопросы кибербезопасности, 2023, 4(56), с. 88–97. DOI:10.21681/2311-3456-2023-4-94-104*
31. *Hariri S., Kind M. C., Brunner R. J. Extended Isolation Forest // IEEE Transactions on Knowledge and Data Engineering, 2021, Vol. 33, No. 4, pp. 1479–1489. DOI: 10.1109/TKDE.2019.2947676*
32. *Murti D. M. P., Pujianto U., Wibawa A. P., Akbar M. I. K-Nearest Neighbor (K-NN) based Missing Data Imputation // 2019 5th International Conference on Science in Information Technology (ICSITech), Yogyakarta, Indonesia, 2019, pp. 83–88. DOI: 10.1109/ICSITech46713.2019.8987530*

33. *Staples L., Ring J., Fontana S., et al. Reproducible clustering with non-Euclidean distances: a simulation and case study // International Journal of Data Science and Analytics, 2023. DOI: 10.1007/s41060-023-00429-1*
34. *Deo T. Y., Sanju A. Data imputation and comparison of custom ensemble models with existing libraries like XGBoost, CATBoost, AdaBoost and Scikit learn for predictive equipment failure // Materials Today: Proceedings, 2023, Volume 72, Part 3, pp. 1596–1604. DOI: 10.1016/j.matpr.2022.09.410*
35. *Barillaro L. Deep Learning Platforms: PyTorch // Reference Module in Life Sciences, Elsevier, 2024. ISBN 9780128096338. DOI: 10.1016/B978-0-323-95502-7.00093-2.S*
36. *S. Mo, W. -H. Chen and X. Lu. Distributed hybrid secondary control strategy for DC microgrid group based on multi-agent system // 2021 33rd Chinese Control and Decision Conference (CCDC), Kunming, China, 2021, pp. 109–114. DOI: 10.1109/CCDC52312.2021.9602249*

INTELLIGENT METHODS OF ENSURING CYBERSECURITY MULTI-AGENT CONTROL SYSTEM OF MICROGRID

Gurina L. A.[3], Tomin N. V.[4]

The research aims *to develop methods for detecting and suppressing the consequences of cyber-attacks in secondary voltage regulation in multi-agent control systems of cyber-physical microgrids.*

The research relies *on the machine learning methods, probabilistic methods.*

Research result: *an isolation forest algorithm for automatic detection of cyber-attacks and an algorithm for data recovery based on the k-nearest neighbors method were developed.*

The scientific novelty *lies in the fact that the proposed method for detecting cyber-attacks and improving information quality creates opportunities for robustness, adaptation and recovery of multi-agent systems in case of cybersecurity breaches.*

Keywords: *cyber-physical microgrid, multi-agent system, intelligent control, identification of cyber-attacks, detection of bad data, improving information quality.*

References

1. *N. Voropai. Electric Power System Transformations: A Review of Main Prospects and Challenges // Energies, 2020, vol. 13(21), 5639. DOI:10.3390/en13215639*
2. *Ilyushin P. V. Sistemnyj podhod k razvitiyu i vnedreniyu raspredelennoj energetiki i vozobnovlyaemyh istochnikov energii v Rossii // Energetik, 2022, 4, s. 20–27.*
3. *Nisha T. N., Pramod D. Sequential pattern analysis for event-based intrusion detection // International Journal of Information and Computer Security, 2019, 11(4/5), 476. DOI:10.1504/ijics.2019.101936*
4. *C. Li, M. Qiu. Reinforcement Learning for Cyber-Physical Systems: with Cybersecurity Case Studies. Chapman and Hall/CRC, 2019.*
5. *S. Gaba et al. A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems // IEEE Access, 2024,* vol. 12, pp. 6017–6035. DOI: 10.1109/ACCESS.2023.3349022
6. *F. O. Olowononi, D. B. Rawat and C. Liu. Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS // in IEEE Communications Surveys & Tutorials, Firstquarter 2021, vol. 23, no. 1, pp. 524–552. DOI: 10.1109/COMST.2020.3036778*
7. *Ilyushin P. V., Vol'nyj V. S. Obzor struktur mikrosetej nizkogo napryazheniya s raspredelennymi istochnikami energii // Relejnaya zashchita i avtomatizaciya [Relay protection and automation]. 2023, № 1(50), s. 68–80.*
8. *Mahela O. P., Khosravy M., Gupta N., et al. Comprehensive Overview of Multi-agent Systems for Controlling Smart Grids // CSEE Journal of Power and Energy Systems, 2022, Vol. 8, No. 1, pp. 115-131. DOI: 10.17775/CSEEJPES.2020.03390*
9. *Jabbar M. A. M., Tran D. T., Kim K. -H. Decentralized Power Flow Control Strategy Using Transition Operations of DC-Bus Voltage for Detection of Uncertain DC Microgrid Operations // Sustainability, 2023, Vol. 15, 11635. DOI: 10.3390/su151511635*
10. *Takayama S., Ishigame A. Volt–Var curve determination method of smart inverters by multi-agent deep reinforcement learning // International Journal of Electrical Power & Energy Systems, 2024, Vol. 157, 109888. DOI: 10.1016/j.ijepes.2024.109888*
11. *Tomin N., Voropai N., Kurbatsky V., Rehtanz C. Management of Voltage Flexibility from Inverter-Based Distributed Generation Using Multi-Agent Reinforcement Learning // Energies, 2021, 14(24), 8270. DOI: 10.3390/en14248270*
12. *Gurina L. A. Ocenka riskov kiberbezopasnosti energeticheskogo soobshchestva mikrosetej // Voprosy kiberbezopasnosti [Cybersecurity issues], 2024, 1(59), s. 101–107. DOI: 10.21681/2311-3456-2024-1-101-107*
13. *H. Zhang, D. Yue, C. Dou and G. P. Hancke/ Resilient Optimal Defensive Strategy of Micro-Grids System via Distributed Deep Reinforcement Learning Approach Against FDI Attack // in IEEE Transactions on Neural Networks and Learning Systems, Jan. 2024, vol. 35, no. 1, pp. 598–608. DOI: 10.1109/TNNLS.2022.3175917*

3 Liudmila A. Gurina, Ph.D. in engineering, Associate Professor, Senior Research Fellow, Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E mail: gurina@isem.irk.ru

4 Nikita N. Tomin, Ph.D. in engineering, Head of Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: tomin.nv@gmail.com

14. *I. Tasevski and K. Jakimoski. Overview of SQL Injection Defense Mechanisms // 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2020, pp. 1-4. DOI: 10.1109/TELFOR51502.2020.9306676*
15. *B. Abazi and E. Hajrizi. Practical analysis on the algorithm of the Cross-Site Scripting Attacks // 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP), Sofia, Bulgaria, 2022, pp. 1-4. DOI: 10.1109/IWSSIP55020.2022.9854491*
16. *Mode, G. R.; Calyam, P.; Hoque, K. A. False data injection attacks in internet of things and deep learning enabled predictive analytics. arXiv 2019, arXiv:1910.01716.*
17. *Y. Gao, H. Hasegawa, Y. Yamaguchi and H. Shimada. Malware Detection by Control-Flow Graph Level Representation Learning With Graph Isomorphism Network // in IEEE Access, 2022, vol. 10, pp. 111830-111841. DOI: 10.1109/ACCESS.2022.3215267*
18. *T. Li, B. Chen, L. Yu and W. -A. Zhang. Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems // in IEEE Transactions on Automatic Control, Sept. 2021, vol. 66, no. 9, pp. 4303-4310. DOI: 10.1109/TAC.2020.3032598*
19. *X. Xie, Y. Liu and B. Xu, Resilient event-triggered control for cyber-physical systems under stochastic-sampling and denial-of-service attacks // 2021 40th Chinese Control Conference (CCC), Shanghai, China, 2021, pp. 4702–4708. DOI: 10.23919/CCC52363.2021.9549917*
20. *A. Talati, V. Garg, N. Mishra, P. Tiwari and P. Jena. Cyber-Attack Detection in Smart Grids Using Machine Learning Approach // 2023 7th International Conference on Computer Applications in Electrical Engineering-Recent Advances (CERA), Roorkee, India, 2023, pp. 1–6. DOI: 10.1109/CERA59325.2023.10455586*
21. *X. Niu, J. Li, J. Sun and K. Tomsovic. Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning // 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2019, pp. 1–6. DOI: 10.1109/ISGT.2019.8791598*
22. *S. Pusarla, U. Ghugar, T. Özseven, B. K. Dewangan, T. Choudhury and J. C. Patni. A Compressive Study on Detection Accuracy Model for DoS Attack in SDN Using Ensemble Learning Techniques // 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), Istanbul, Turkiye, 2023, pp. 1–6. DOI: 10.1109/ISAS60782.2023.10391345*
23. *A. Srivastava, H. S. Sharma, R. Rawat and N. Garg. Detection of Cyber Attack in IoT Based Model Using ANN Model with Genetic Algorithm // 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 1198–1201. DOI: 10.1109/IC2PCT60090.2024.10486578*
24. *A. AlBusaidi and F. H. Mohideen. Analysis of Wireless Sensor Network Security Models: A Salient Approach for Deeper Inspection Using Deep Neural Networks // 2023 International Conference on Emerging Techniques in Computational Intelligence (ICETCI), Hyderabad, India, 2023, pp. 276–282. DOI: 10.1109/ICETCI58599.2023.10330927*
25. *S. Puneeth, S. Lal, M. Pratap Singh and B. S. Raghavendra. RMDNet-Deep Learning Paradigms for Effective Malware Detection and Classification // in IEEE Access, 2024, vol. 12, pp. 82622-82635, 2024. DOI: 10.1109/ACCESS.2024.3403458*
26. *P. S. Patil, S. L. Deshpande, G. S. Hukkeri, R. H. Goudar and P. Siddarkar. Prediction of DDoS Flooding Attack using Machine Learning Models // 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1–6. DOI: 10.1109/ICSTCEE56972.2022.10100083*
27. *S. Bala and S. M. M. Ahsan. Detecting DDoS attacks in Software Define Networking: A Machine Learning Based Approach // 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM), Gazipur, Bangladesh, 2023, pp. 1–6. DOI: 10.1109/NCIM59001.2023.10212569*
28. *Sarker I. H. Machine Learning: Algorithms, Real-World Applications and Research Directions // SN Computer Science, 2021, 2(3). DOI:10.1007/s42979-021-00592-x*
29. *Ripan Rony, Md. Moinul Islam, Alqahtani Hamed, Sarker Iqbal H. Effectively predicting cyber-attacks through isolation forest learning-based outlier detection // Security and Privacy, 2022, 5(3). DOI:10.1002/spy2.212*
30. *Gurina L. A., Tomin N. V. Razrabotka kompleksnogo podhoda k obespecheniyu kiberbezopasnosti vzaimosvyazannyh informacionnyh sistem pri intellektual'nom upravlenii soobshchestvom mikrosetej // Voprosy kiberbezopasnosti [Cybersecurity issues], 2023, 4(56), s. 88–97. DOI:10.21681/2311-3456-2023-4-94-104*
31. *Hariri S., Kind M. C., Brunner R. J. Extended Isolation Forest // IEEE Transactions on Knowledge and Data Engineering, 2021, Vol. 33, No. 4, pp. 1479–1489. DOI: 10.1109/TKDE.2019.2947676*
32. *Murti D. M. P., Pujianto U., Wibawa A. P., Akbar M. I. K-Nearest Neighbor (K-NN) based Missing Data Imputation // 2019 5th International Conference on Science in Information Technology (ICSITech), Yogyakarta, Indonesia, 2019, pp. 83-88. DOI: 10.1109/ICSITech46713.2019.8987530*
33. *Staples L., Ring J., Fontana S., et al. Reproducible clustering with non-Euclidean distances: a simulation and case study // International Journal of Data Science and Analytics, 2023. DOI: 10.1007/s41060-023-00429-1*
34. *Deo T. Y., Sanju A. Data imputation and comparison of custom ensemble models with existing libraries like XGBoost, CATBoost, AdaBoost and Scikit learn for predictive equipment failure // Materials Today: Proceedings, 2023, Volume 72, Part 3, pp. 1596–1604. DOI: 10.1016/j.matpr.2022.09.410*
35. *Barillaro L. Deep Learning Platforms: PyTorch // Reference Module in Life Sciences, Elsevier, 2024. ISBN 9780128096338. DOI: 10.1016/B978-0-323-95502-7.00093-2.S*
36. *S. Mo, W. -H. Chen and X. Lu. Distributed hybrid secondary control strategy for DC microgrid group based on multi-agent system // 2021 33rd Chinese Control and Decision Conference (CCDC), Kunming, China, 2021, pp. 109-114. DOI: 10.1109/CCDC52312.2021.9602249*