УДК 004.056

ПРОГНОЗИРОВАНИЕ АТАК НА ПОДСИСТЕМУ УПРАВЛЕНИЯ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ

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

А.В. Ярмак
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: yarmak.av@ibks.spbstu.ru

Ключевые слова: прогнозирование, многомерные временные ряды, глубокое обучение, нейронные сети

Аннотация: Предложен подход к обнаружению нарушений информационной безопасности в автоматизированных системах управления технологическими процессами (АСУ ТП), заключающийся в прогнозировании многомерных временных рядов, сформированных из значений параметров работы конечных устройств системы. С использованием экспериментального макета очистки воды произведено сравнение результатов прогнозирования для параметров, характеризующих работу всего макета, и для параметров, характеризующих протекание отдельных подпроцессов, реализуемых макетом. Для прогнозирования выполнялось обучение GRU-нейронной сети.

1. Введение

Повышение конкурентоспособности производственного сектора за счет применения интеллектуальных технологий, обеспечивающих автономность работы промышленных систем от человека, является ключевой задачей долгосрочной стратегии развития промышленности для многих стран (Германия, США, Япония и т.д.) [1]. Интеграция интеллектуальных технологий с промышленными объектами привела к тому, что многие компоненты таких систем стали доступны из сети Интернет. Это стало причиной роста числа кибератак на промышленные объекты [2-4]. При этом, наблюдается тенденция к получению злоумышленниками доступа к подсистеме управления промышленными объектами.

Последствия успешной реализации кибератак на такие объекты могут быть катастрофическими, вплоть до нанесения непоправимого ущерба экологии и гибели людей. Поскольку многие промышленные объекты интегрированы с критическими отраслями деятельности, для них необходимо обеспечить раннее обнаружение кибератак или их предотвращение. Учитывая связь подсистемы управления промышленных объектов как

с сетевыми устройствами, так и с управляемыми конечными устройствами, которые могут быть доступны из сети Интернет, необходимо обнаруживать атаки на подсистему управления с обеих сторон.

Для защиты сетевого периметра промышленных объектов используются различные механизмы обеспечения безопасности, однако в редких случаях промышленный объект включает в состав защитных механизмов средство, обеспечивающее контроль функционирования компонентов нижнего уровня. Разработка и внедрение такого средства представляет определенные сложности в связи с разнородностью конечных устройств и их малой мощностью.

Для решения данной проблемы предлагается осуществлять мониторинг данных от конечных устройств промышленных объектов и представлять поступающие данные в виде многомерного временного ряда. Раннее обнаружение атак предлагается обеспечивать за счет прогнозирования многомерного временного ряда с использованием нейросетевых технологий.

2. Описание предлагаемого подхода к прогнозированию многомерных временных рядов

Современные промышленные объекты включают в себя многочисленные контуры управления, пользовательские интерфейсы, средства удаленной диагностики и обслуживания, построенные с использованием множества сетевых протоколов на многоуровневых сетевых архитектурах. Используемые подходы к обеспечению безопасности промышленных объектов включают сегментацию сети, защиту границ доменов безопасности, использование межсетевых экранов и систем обнаружения вторжений, средств аутентификации. Однако, большинство этих подходов направлено на защиту сетевого периметра объекта, и для защиты компонентов нижнего уровня – программируемых логических контроллеров, сенсоров и актуаторов – они не будут эффективными. При этом, следует отметить, что значительное число атак на подсистему управления промышленных объектов производится именно с использованием компонентов нижнего уровня системы. Следовательно, необходим подход, обеспечивающий раннее обнаружение атак путем анализа данных от компонентов нижнего уровня промышленных объектов.

Для обнаружения аномалий предлагается собирать данные со всех компонентов нижнего уровня и представлять их в виде многомерного временного ряда. Такой подход позволит получить представление о функционировании и динамике всего промышленного объекта в целом, в соответствии с принципом Sensor Fusion. В соответствии с источником [5], Sensor Fusion представляет собой объединение данных от различных сенсоров системы таким образом, что полученная в результате анализа объединенных данных информация в некотором смысле лучше, чем информация, полученная от каждого из сенсоров по отдельности. Под термином «лучше» авторы подразумевают большую информативность и значимость для дальнейшего анализа, в данном случае – для анализа безопасности.

3. Описание экспериментального макета и выбор архитектуры нейронной сети

Для проведения экспериментальных исследований взят испытательный стенд SWaT, который представляет собой уменьшенную версию системы автоматической очистки воды [6]. Процесс очистки воды состоит из шести процессов, обозначаемых P1-P6. Каждый из этих процессов управляется набором из двух ПЛК – основного и резервного. В состав макета входит 51 устройство (сенсоры и актуаторы), общее число устройств распределено по всем подпроцессам. Таким образом, каждая точка временного ряда имеет размерность 51 и позволяет уловить шаблоны, характеризующие стандартное поведение системы.

При выборе архитектуры нейронной сети, был проведен анализ исследовательских работ, связанных с обнаружением и прогнозированием аномалий во временных рядах. Большинство работ сосредоточено на анализе одномерных временных рядов и применении аппарата математической статистики [7-9]. Однако эффективность нейросетевых технологий в задаче предсказания временных рядов, в том числе, многомерных, привела к появлению новых методов, направленных на раннее обнаружение сетевых атак.

В работе предлагается использовать рекуррентные GRU-нейронные сети, их выбор обусловлен хорошими результатами, полученными путем их применения в задаче прогнозирования временных рядов. Используемая модель нейронной сети включает в себя два GRU-слоя и полносвязный слой, а для регуляризации сети и предотвращения переобучения используются слои дропаута с вероятностью, равной 0,2. Для обучения сети без учителя использовались данные, соответствующие нормальному функционированию макета.

4. Экспериментальные исследования

При проведении экспериментальных исследований было выдвинуто предположение о том, что для промышленных объектов большую эффективность позволит получить прогнозирование многомерных временных рядов, описывающих отдельные подпроцессы, чем прогнозирование одного многомерного временного ряда, описывающего функционирование объекта в целом. В связи с этим, прогнозирование проводилось двумя способами.

При анализе единого многомерного временного ряда, характеризующего работу всего макета, точность сети на тренировочных данных составила 90%, на валидационном множестве − 82%, значение среднеквадратичной ошибки MSE – 0,06 и 0,03 соответственно. На рис. 1 представлен пример работы модели предсказания на основе нейронной сети для значений, взятых из тестовой выборки.

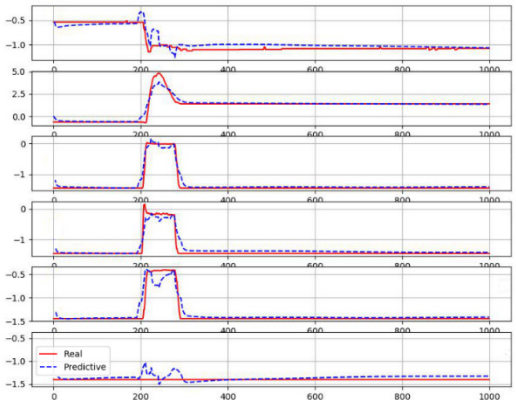

Рис. 1. Предсказание временных рядов с помощью рекуррентной сети.

Аномалии в данных датчиков представляют собой отклонения от стандартных, предсказанных шаблонов функционирования системы. Для выявления подобных отклонений строится вектор ошибки, характеризующий разность между текущими показателями, полученными от объектов системы, и предсказанными значениями. Анализ ошибки предсказания направлен на выявление аномалий: чем большее значение имеет какая-либо компонента, тем выше вероятность того, что имеет место атака или сбой в системе. На рис. 2 представлен график ошибки предсказания при атаках на макет.

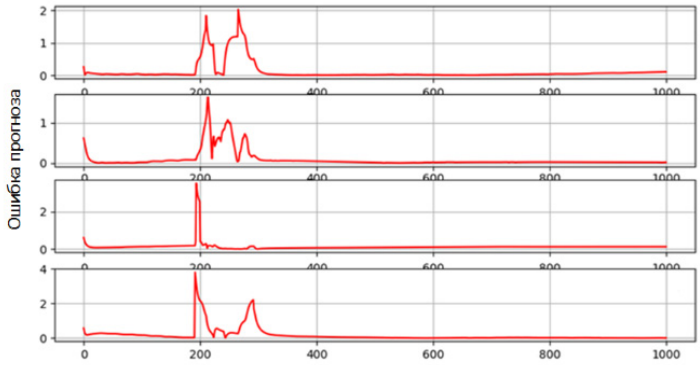

Рис. 2. График ошибки предсказания при атаках на систему.

Порог ошибки прогноза определялся экспериментально. При значении порога в 0,6 доля обнаруженных аномалий составила около 85%.

Для прогнозирования многомерных временных рядов, характеризующих каждый из шести подпроцессов очистки воды, реализуемых макетом, потребовал обучения шести нейронных сетей. Однако, при обучении одной нейронной сети для прогнозирования многомерного временного ряда потребовалось около 15 часов, а совокупное время при обучении шести нейронных сетей оказалось меньше – 12 часов. При этом, во втором случае существует возможность распараллелить обучение нейронных сетей, в результате чего время обучения сократится в несколько раз, примерно до 2 часов. Результаты прогнозирования для процесса P2 представлены на рис. 3.

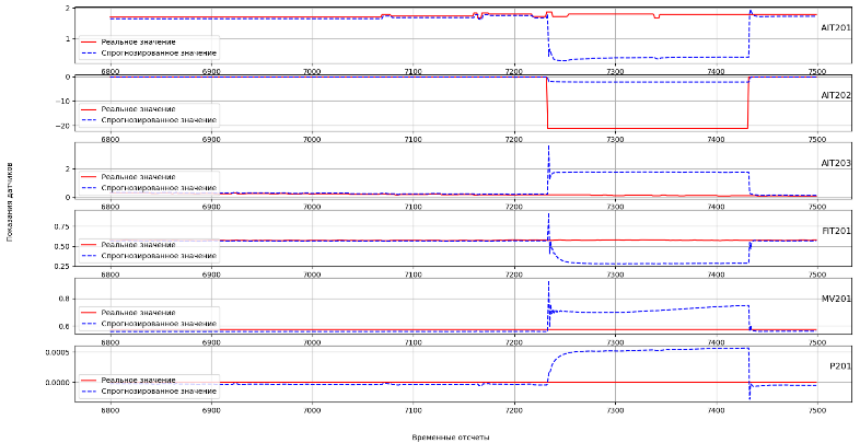

Рис. 3. График ошибки предсказания при атаках на систему.

При этом, точность сети на тренировочных данных значительно увеличилась и составила порядка 94%, как и на валидационном множестве. Среднеквадратичная ошибка MSE равна 0,008 и 0,002 соответственно.

5. Заключение

Экспериментальные исследования предложенного подхода к прогнозированию многомерных временных рядов, сформированных из значений показателей устройств нижнего уровня промышленных объектов продемонстрировали высокую эффективность – большинство смоделированных атак, направленных на внесение изменений в работу подсистемы управления, было обнаружено на ранней стадии. Следует отметить тот факт, что при агрегировании данных от компонентов промышленного объекта объединение данных по подпроцессам, реализуемым промышленным объектом, достигается выигрыш в скорости при обучении нейронной сети, а также увеличивается точность прогнозирования.

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

Результаты работы получены с использованием вычислительных ресурсов суперкомпьютерного центра Санкт-Петербургского политехнического университета Петра Великого – СКЦ «Политехнический» (http://www.spbstu.ru).

Список литературы

1. Как устроен умный завод. https://iot.ru/promyshlennost/kak-ustroen-umnyy-zavod/.
2. Васильев Ю.С., Зегжда Д.П., Зегжда П.Д. Обеспечение безопасности автоматизированных систем управления технологическими процессами на объектах гидроэнергетики // Известия РАН. Секция Энергетика. 2016. № 3. С. 22.
3. Bakhshi Z., Balador A., Mustafa J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models // Wireless Communications and Networking Conference Workshops (WCNCW), 2018. P. 173-178.
4. Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы, 2017. № 3. С. 9-23.
5. Elmenreich W. An introduction to sensor fusion // Vienna University of Technology, Austria, 2002. Vol. 502. P. 1-28.

6. Secure Water Treatment Testbed (SWaT): An Overview. https://itrust.sutd.edu.sg/wp-content/uploads/sites/3/2015/11/Brief-Introduction-to-SWaT_181115.pdf.
7. Tulone D., Madden S. PAQ: Time series forecasting for approximate query answering in sensor networks // European Workshop on Wireless Sensor Networks, 2006. P. 21-37.
8. Wei L., Kumar N., Lolla V., Keogh E., Lonardi S., Ratanamahatana C. Assumption-Free Anomaly Detection in Time Series // SSDBM, 2005. Vol. 5. P. 237-242.
9. Pincombe B. Anomaly detection in time series of graphs using ARMA processes // Asor Bulletin. 2005. Vol. 24, No, 4. P. 2.