УДК 004.896 + 004.056.5 Вестник УрФО № 2(32) / 2019, с. 60–65

Алабугин С. К., Пятницкий И. А., Соколов А. Н.

DOI: 10.14529/secur190209

ПРИМЕНЕНИЕ РЕКУРРЕНТНЫХ И СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Рассмотрены вопросы применимости методов машинного обучения в задаче обнаружения аномалий технологического процесса. Описаны причины, по которым возникла эта задача, а также предпосылки использования методов машинного обучения для её решения. На примере набора данных New Gas Pipeline проведен анализ источников по вопросу применимости различных методов машинного обучения. В результате анализа источников выявлен ряд недостатков, не позволяющих использовать для выявления аномалий технологического процесса классические алгоритмы классификации, кластеризации и обнаружения аномалий. В качестве перспективного способа решения задачи были выбраны методы на основе рекуррентных и сверточных нейронных сетей, а также намечены основные направления дальнейших исследований в этой области.

Ключевые слова: *Обнаружение вторжений, автоматизированная система управления технологическим процессом (АСУ ТП), выявление аномалий, машинное обучение, глубокое обучение, рекуррентные нейронные сети.*

Sokolov A. N., Alabugin S. K., Pyatnitsky I. A

APPLYING OF RECURRENT AND CONVOLUTIONAL NEURAL NETWORKS FOR ANOMALY DETECTION OF INDUSTRIAL PROCESS

The questions of the machine learning methods applicability in the anomaly detection of

the industrial process are considered. The reasons for which this problem arose are described, as well as the prerequisites for machine learning methods usage. The analysis of the sources was carried out on the applicability of various methods of machine learning using the example of the New Gas Pipeline dataset. As a result of the analysis of the sources, a number of shortcomings, which do not allow the classical classification, clustering and anomaly detection algorithms to be used to detect process anomalies, were revealed. The classes of models based on recurrent and convoutional neural networks was chosen as a promising method for solving the problem, and the main directions for further research in this area were outlined.

Keywords: *Intrusion detection, industrial Control System (ICS), anomaly detection, machine learning, deep learning, recurrent neural networks.*

Современная автоматизированная система управления технологическими процессами (АСУ ТП) является не только информационной, но и физической системой, в которой присутствует программное и аппаратное обеспечение для управления технологическими процессами. По этой причине, атаки злоумышленников, направленные на АСУ ТП, несут большую угрозу [1] в силу своих возможных последствий: остановка производства, выведение оборудования из строя, техногенные катастрофы.

В течение долгого времени главным средством защиты АСУ ТП была их изолированность от любых внешних сетей, однако в настоящий момент наблюдается тенденция к объединению индустриальных и технологических сетей. Это, а также отсутствие культуры информационной безопасности, делает АСУ ТП уязвимыми для атак злоумышленников.

Некоторые АСУ ТП, размещенные на промышленных предприятиях, могут относиться к объектам критической информационной инфраструктуры. По этой причине, злоумышленники проводят целевые атаки на подобные объекты и, не всегда такую атаку могут обнаружить классические системы обнаружения вторжений, применяющие сигнатурный поход. Поэтому для обнаружения вторжений предлагается использовать подход, основанный на выявлении аномалий.

Атаки, направленные на АСУ ТП, могут проявляться через нехарактерное поведение как устройств, составляющих сетевую инфраструктуру, так и оборудования, которое непосредственно участвует в технологическом процессе. В качестве примера можно привести аномальное изменение показаний датчиков или изменение сценариев работы контроллеров. Подобное поведение может являться следствием перепрошивки логики управления, спуфинга данных сенсоров, отказа в обслуживании и иных атак. По вышеперечисленным причинам для обнаружения атак целесообразно использовать не только средства, ориентированные на обнаружение вторжений в корпоративных системах и сетях, но и отслеживать состояние технологического процесса через его параметры.

Технологический процесс имеет значительное количество параметров, нормативные значения которых могут изменяться при изменении структуры процесса, неизбежно происходящее со временем. Кроме того, сигналы датчиков технологического оборудования, как правило, взаимосвязаны и могут быть зашумлены вследствие воздействия помех. Наличие взаимосвязей и шумов значительно усложняет задачу обнаружения аномалий в работе АСУ ТП. Поэтому, для выявления аномалий в работе технологического процесса, предлагается использовать методы машинного обучения, позволяющие избежать создания большого числа правил, регламентирующих нормальную работу процесса.

Как правило, задачу обнаружения вторжений пытаются свести к одной из общих задач, решаемых машинным обучением: классификации, кластеризации или обнаружению аномалий. В качестве примера, рассмотрим результаты, полученные при исследованиях на наборе данных New Gas Pipepline [2].

Набор данных New Gas Pipeline собран в ходе логгирования сетевого трафика лабораторной SCADA-системы. В нём представлены данные, соответствующие нормальной работе системы и данные, соответствующие различным атакам. Смоделированная таким образом система состоит из:

- бензопровода с помпой, соединенного с компрессором,
- датчика давления,
- предохранительного клапана, управляемого соленоидом.

Необходимый уровень давления в системе поддерживается с помощью пропорционально-интегрально-дифференцирующего (ПИД) регулятора. Для коммуникации в описанной системе используется протокол прикладного уровня Modbus. Сетевые пакеты с метками времени после некоторой обработки составляют набор данных. В табл.1 представлены признаки набора данных. Каждая строка набора данных соответствует либо нормальному состоянию, либо одному из семи видов атак. Общий объем набора данных составляет 274628 записей, из которых 214580 соответствуют нормальному состоянию системы и 60048 – какой-либо из атак.

представлены в табл. 2. Для оценки результатов используется несколько метрик: доля правильных ответов алгоритма, точность (precision) и полнота (recall).

Под *точностью* понимается отношение количества объектов, которые правильно помечены классификатором как объекты некоторого класса *A* к общему количеству объектов, помеченных классификатором как объект класса *A*. *Полнота* – это отношение количества объектов, которые правильно помечены классификатором как объекты некоторого класса *A* к количеству всех объектов, составляющих класс *A*.

Представленные результаты получены в

Таблица 1

Признаки набора данных New Gas Pipeline

Признак	Описание
addres	Адрес станции
crc rate	Значение контрольной суммы пакета
function	Код Modbus функции
length	Длина пакета Modbus
setpoint	Установленное значение давления
gain	Коэффициент передачи ПИД
reset rate	Частота сброса ПИД
deadband	Зона нечувствительности ПИД
cycle time	Время цикла ПИД
rate	Коэффициент усиления ПИД
system mode	Режим работы: автоматический (2), ручной(1) или выкючен (0)
control scheme	Контроль давления с помощью помпы (0) или соленоида(1)
pump	Помпа открыта (1) или закрыта(0)
solenoid	Клапан открыт (1) или закрыт (0)
pressure measurement	Значение давления в бензопроводе
command response	Пакет содержит команду (1) или ответ (0)
Time	Метка времени

Таблица 2

Результаты работы различных алгоритмов на наборе данных New Gas Pipeline

Алгоритм	Доля правильных ответов алгоритма	Точность	Полнота
Сеть Байеса	0.87	0.97	0.59
Support Vector Data Description	0.76	0.95	0.21
Isolation Forest	0.70	0.51	0.13
K-means	0.57	0.83	0.57
Gaussian Mixture Model	0.45	0.79	0.44
Principal Component Analysis with Singular Value Decomposition	0.17	0.65	0.28

В ходе анализа работ [3, 4] можно увидеть, насколько различные методы машинного обучения применимы для выявления атак (на описанном наборе данных). Результаты

случае, когда в наборе данных выделено всего два класса: нормальная активность и аномалия. Как видно из табл. 2, алгоритмы классификации (сеть Байеса, Support Vector Data

Description и K-means) лучше справляются с задачей, доля правильных ответов выше и точность выше, чем у алгоритмов кластеризации (Gaussian Mixture Model и Principal Component Analysis with Singular Value Decomposition) и алгоритма обнаружения аномалий (Isolation Forest). Это можно объяснить тем, что алгоритмы кластеризации и обнаружения аномалии основаны на понятиях кластера и аномалии, соответственно. В настоящее время не существует полного понимания того, как определить понятие аномалии, чтобы оно соответствовало атаке, и как осуществлять поиск кластеров в данных, чтобы один или несколько из них точно соответствовали атакам. Поэтому, классические алгоритмы кластеризации и обнаружения аномалий плохо применимы на практике для выявления аномалий технологических процессов и в работе АСУ ТП в целом. Если рассматривать классические алгоритмы классификации, возникает вопрос: достаточно ли хорошо классификатор обучился определять нормальное состояние и распознает ли он новую атаку, если соответствующих ей примеров не было в обучающей выборке?

Одним из способов преодоления этих противоречий является использование рекуррентных нейронных сетей [5]. Рекуррентные нейронные сети являются одной из разновидностей архитектур нейронных сетей, отличительной особенностью которых является наличие обратной связи, что позволяет им анализировать последовательные данные (временные ряды). С помощью рекуррентной нейронной сети можно анализировать ход технологического процесса, обучая сеть данными, полученными с датчиков и сенсоров АСУ ТП. Анализируя технологический процесс как последовательность измерений его различных параметров, сеть научится предсказывать его состояние в следующий момент времени. Таким образом, в случае, когда предсказанное нейронной сетью состояние отличается от текущего, регистрируется аномалия. В качестве примера эффективности рекуррентных нейронных сетей можно привести подход, описанный в работе [3]. Авторы предлагают последовательно использовать фильтр Блума [6] для выявления аномалий в содержимом пакета Modbus, а затем, в случае не выявления аномалии, рекуррентную нейронную сеть архитектуры Long Short-Term Memory (LSTM). Используя предложенный подход, удалось добиться хороших результатов: доля правильных ответов алгоритма составила 0.92, точность – 0.94, полнота – 0.78. Таким образом, подход, предложенный авторами, оказался лучше иных алгоритмов по двум метрикам из трёх.

Стоит заметить, что помимо рекуррентных нейронных сетей для анализа и прогнозирования временных рядов могут использоваться сверточные нейронные сети (convolutional neural networks). Они не имеют рекуррентных связей между слоями и используют операцию свертки, что также позволяет использовать их для выявления аномалий технологического процесса. В качестве примера можно привести работу [8], в которой исследователи применяли сверточные нейронные сети для обнаружения аномалий в работе процесса очищения воды. Полученные результаты свидетельствуют о том, что сверточные нейронные сети могут с успехом применяться в рамках этой задачи.

Подводя итоги, можно говорить о том, что применение рекуррентных и сверточных нейронных сетей перспективно в задаче прогнозирования временных рядов при обнаружении аномалий в работе АСУ ТП и технологического процесса. На основании результатов работ [3, 8] можно предположить следующие направления исследований в этой области:

- исследование новых архитектур рекуррентных нейронных сетей, в частности сетей, использующих Gated Recurrent Unit (GRU) [7];
- поиск новых решений, не основанных на сборе базы сигнатур, соответствующих атакам (фильтров Блума), – таких, например, как разработка новых информативных признаков (feature engineering) для нейронной сети с использованием классических методов обнаружения аномалий;
- применение и тестирование сверточных нейронных сетей на больших данных.

Литература

1. Баринов А. Е., Скурлаев С. В., Соколов А. Н. Методика оценки рисков, вызванных уязвимостями в программном обеспечении автоматизированных систем управления технологическими процессами //Вестник УрФО. Безопасность в информационной сфере. – 2017. – №. 3. – С. 34-42.

2. Morris T. H., Thornton Z., Turnipseed I. Industrial control system simulation and data logging for

intrusion detection system research //Proceedings of the Seventh Annual Southeastern Cyber Security Summit. – 2015.

3. Feng C., Li T., Chana D. Multi-level anomaly detection in industrial control systems via package signatures and lstm networks //Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on. – IEEE, 2017. – C. 261-272.

4. Shirazi S. N. et al. Evaluation of anomaly detection techniques for scada communication resilience // Resilience Week (RWS), 2016. – IEEE, 2016. – C. 140-145.

5. Lipton Z. C., Berkowitz J., Elkan C. A critical review of recurrent neural networks for sequence learning //arXiv preprint arXiv:1506.00019. – 2015.

6. Parthasarathy S., Kundur D. Bloom filter based intrusion detection for smart grid SCADA //Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on. – IEEE, 2012. – C. 1-6.

7. Cho K. et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation //arXiv preprint arXiv:1406.1078. – 2014.

8. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks //Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. – ACM, 2018. – C. 72-83.

References

1. Barinov A. E., Skurlaev S. V., Sokolov A. N. Metodika otsenki riskov, vyzvannykh uyazvimostyami v programmnom obespechenii avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2017. – no. 3. – pp. 34-42.

2. Morris T. H., Thornton Z., Turnipseed I. Industrial control system simulation and data logging for intrusion detection system research //Proceedings of the Seventh Annual Southeastern Cyber Security Summit. – 2015.

3. Feng C., Li T., Chana D. Multi-level anomaly detection in industrial control systems via package signatures and lstm networks //Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on. – IEEE, 2017. – C. 261-272.

4. Shirazi S. N. et al. Evaluation of anomaly detection techniques for scada communication resilience //Resilience Week (RWS), 2016. – IEEE, 2016. – C. 140-145.

5. Lipton Z. C., Berkowitz J., Elkan C. A critical review of recurrent neural networks for sequence learning //arXiv preprint arXiv:1506.00019. – 2015.

6. Parthasarathy S., Kundur D. Bloom filter based intrusion detection for smart grid SCADA //Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on. – IEEE, 2012. – C. 1-6.

7. Cho K. et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation //arXiv preprint arXiv:1406.1078. – 2014.

8. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks //Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. – ACM, 2018. – C. 72-83.

АЛАБУГИН Сергей Константинович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sergei_alabugin@mail.ru

ПЯТНИЦКИЙ Илья Альбертович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: Ankidoom@gmail.com

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

ALABUGIN Sergei, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University

(national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sergei_alabugin@mail.ru

PYATNITSKY Ilya, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: Ankidoom@gmail.com

SOKOLOV Alexander, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru