Евгений В. Андрюхин[1], Михаил К. Ридли[2]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: andryukhin@gmail.com, https://orcid.org/0000-0001-6876-0960
[2]Московский авиационный институт,
Волоколамское ш., 4, г. Москва, 125993, Россия
e-mail: mr@kalabi.ru, https://orcid.org/0000-0003-2158-6277

АНАЛИЗ СЕТЕВОГО ТРАФИКА ДЛЯ ВЫЯВЛЕНИЯ КРИТИЧЕСКИХ СОСТОЯНИЙ СИСТЕМ АВТОМАТИЗАЦИИ В УСЛОВИЯХ ИНДУСТРИАЛЬНЫХ ПРОМЫШЛЕННЫХ СЕТЕЙ

DOI: http://dx.doi.org/10.26583/bit.2018.3.08

Аннотация. Промышленные сети являются одной из важнейших частей системы управления производственными процессами - MES-системы. Используя такие сети, MES-системы решают задачи синхронизации, координации процессов, а также оптимизируют выпуск продукции в рамках производства. Задачи назначаются в соответствии с загруженностью на исполнительных объектах - программируемых логических контроллерах (ПЛК), чья основная цель функционирования состоит в качественном выполнении поставленной задачи. Каждый ПЛК обладает набором значений, которые могут быть как прочитаны, так и перезаписаны. Процесс чтения и перезаписи выполняется часто, например, каждые 50-150 миллисекунд, что позволяет получать большие наборы данных для исследования за короткий промежуток времени. Наборы данных представляются в виде временного ряда, таким образом, состояния системы оказываются упорядочены относительно выбранных моментов времени через равные промежутки. Информация, полученная в такие моменты времени, может предоставить возможность как для построения предположений о текущем состоянии системы, так и о возможных изменениях состояния в течение нескольких следующих шагов. Предлагаемый подход позволяет выявить критические состояния на основе анализа сетевого трафика с целью предотвращения возможности появления аномалий во всей системе и помочь оператору индустриальных систем минимизировать ущерб, который мог быть вызван отказом системы. Целью работы являлось выделение характеристик промышленного трафика, на основе которых выявление состояний системы в различные моменты времени при помощи алгоритмов кластеризации наиболее эффективно. Используя набор данных, полученный в течение работы тестового стенда процесса АСУ ТП по переработке нефти, а также набора аномальных событий, полученных вследствие атак на стенд АСУ ТП, была разработана тестовая выборка для обучения системы. В результате работы были выделены ключевые характеристики трафика, которые позволяют разделять состояния системы наиболее точно.

Ключевые слова: промышленные сети, анализ трафика, информационная безопасность, машинное обучение, выявление аномалий.
Для цитирования: АНДРЮХИН, Евгений В.; РИДЛИ, Михаил К. АНАЛИЗ СЕТЕВОГО ТРАФИКА ДЛЯ ВЫЯВЛЕНИЯ КРИТИЧЕСКИХ СОСТОЯНИЙ СИСТЕМ АВТОМАТИЗАЦИИ В УСЛОВИЯХ ИНДУСТРИАЛЬНЫХ ПРОМЫШЛЕННЫХ СЕТЕЙ. Безопасность информационных технологий, [S.l.], n. 3, p. 79-87, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1142>. Дата доступа: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.08.

Evgeny V. Andryukhin[1], Mihail K. Ridli[2]
[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: andryukhin@gmail.com, https://orcid.org/0000-0001-6876-0960
[2]Moscow Aviation Institute,
Volokolamskoe shosse, 4, Moscow, 125993, Russia
e-mail: mr@kalabi.ru, https://orcid.org/0000-0003-2158-6277

A network traffic analysis for critical automation system state detection in industrial networks

DOI: http://dx.doi.org/10.26583/bit.2018.3.08

Abstract. Industrial networks are one of the most important parts of the manufacturing execution system. Via these networks, it is possible to allocate tasks according to the network components load. Each network component - programming logic controller (PLC) has its set of parameter values, which can be read or even rewritten. The reading or writing process can be performed very often, for example, every 50-150 milliseconds. It allows collecting a huge amount of datasets for research purposes in a very short time. The datasets are represented as a time series, so the system states are ordered with respect to the selected moments of time at equal intervals. The information collected at these moments of time can provide an opportunity to make assumptions about the current state of the system, as well as about possible changes of state in the next few steps. The proposed approach allows detecting a critical system states via network traffic analysis without deep traffic inspection, to stop anomalies spread in the system, and to decrease the possible amount of harm to the system. The main goal of the present study is to obtain a set of industrial traffic parameters, which can be used to detect system state at any moment of time using machine learning clustering methods efficiently. Using a dataset obtained during the operation of the test oil-refinery stand as well as a set of anomalous events obtained as a result of attacks on the stand, a test sample was developed for training the system. As a result of this work, the key characteristics of traffic were identified, which allow to detect the system states in the most accurate way.
Keywords: industrial networks, traffic analysis, information security, machine learning, anomalies detection.
For citation: ANDRYUKHIN, Evgeny V.; RIDLI, Mihail K. A network traffic analysis for critical automation system state detection in industrial networks. IT Security (Russia), [S.l.], n. 3, p. 79-87, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1142>. Date accessed: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.08.

Введение

Промышленные сети являются одной из важнейших частей системы управления производственными процессами - MES-системы. Используя такие сети, MES-система решает задачи синхронизации, координирует и оптимизирует выпуск продукции в рамках производства. Задачи назначаются в соответствии с загруженностью на исполнительных сетевых объектах - программируемых логических контроллерах (ПЛК), чья основная цель и состоит в качественном выполнении поставленной задачи. Каждый ПЛК обладает набором значений, которые могут быть как прочитаны, так и перезаписаны. Процесс чтения и перезаписи выполняется часто, например, каждые 50-150 миллисекунд. Такое частое выполнение операций позволяет сделать прогноз более точным вследствие большого набора статистического материала на каждом из ПЛК.

В большинстве случаев промышленные сети делятся на две подсети: внутреннюю и внешнюю. Внутренняя сеть, которая функционирует между ПЛК и системами диспетчерского управления и сбора данных (SCADA-системами), использует собственные протоколы для коммуникации. Внешняя сеть использует традиционный сетевой TCP/IP стек, иногда инкапсулируя его в GPRS [1] для передачи данных от полевых устройств, расположенных далеко от SCADA-системы [2].

Несмотря на то, что промышленные сети часто используют сетевой TCP/IP стек, протоколы существенно различаются между собой и не решают задач по защите передаваемых данных. Например, такие широко распространенные протоколы как Goose [3] и Modbus [4], которые предлагаются в МЭК 61850, не используют шифрование или цифровую подпись для защиты передаваемых данных. Этот факт вынуждает компании создавать собственные сетевые коммуникационные протоколы, например, S7Comm, реализованный компанией Siemens в исполнении для устройств Simatic S7, протокол в версии ПЛК, большей чем 1200, использует шифрование, однако не удовлетворяет требованиям МЭК 61850 по скорости передачи данных для поддержания достаточного уровня аварийной защиты [5]. Таким образом, перед компаниями стоит задача разработки новых или адаптации существующих сетевых протоколов для защиты передаваемых данных без нарушения требований МЭК.

Аномалией здесь и далее будет называться исключение, которое может быть определено как отклонение от типичного или ожидаемого поведения. Поскольку автоматизированные системы управления технологическим процессом (АСУ ТП) должны

быть стабильными и иметь предсказуемое поведение, то проактивное обнаружение аномалий может быть полезным для выявления отказов системы.

Предлагаемый подход позволяет выявить критические состояния на основе анализа сетевого трафика с целью предотвращения возможности появления аномалий во всей системе и помочь оператору SCADA-системы минимизировать ущерб, который мог быть вызван отказом системы. Используя набор данных, полученный в течение работы тестового стенда процесса АСУ ТП по переработке нефти, а также набор аномальных событий, полученных вследствие атак на стенд АСУ ТП, была разработана тестовая выборка для обучения системы.

Формулировка проблемы

МЭК 61850 является стандартом, описывающим форматы потоков данных, виды информации, правила описания элементов энергообъекта и свод правил для организации событийного протокола передачи данных [6]. Эти правила требуют от промышленных систем иметь должный уровень отказоустойчивости и достаточно высокую скорость передачи данных. Для того чтобы удовлетворять всем требованиям по безопасному функционированию промышленных процессов, архитекторы таких систем вынуждены пренебрегать функциями обеспечения кибербезопасности, такими как, например, криптография. Такой недостаток механизмов безопасности ставит задачу своевременного обнаружения атак на систему. Для раздельных серверов (например, SCADA-сервера и сервера хранения истории) и локальных сетей такая задача решается путем внедрения систем обнаружения вторжений (СОВ) или систем предотвращения вторжений одновременно с системой сбора и корреляции событий ИБ [7]. Однако в промышленных сетях такой подход применить невозможно в силу того, что для анализа событий используется сигнатурный подход, который часто неприменим к АСУ ТП сегменту по причине специфики как оконечного оборудования и программного обеспечения, так и типа передаваемых данных [8]. Принимая во внимание большое количество новостных сообщений об обнаружениях уязвимостей "нулевого" дня для различного программного обеспечения на различных платформах, поднимается задача разработки удовлетворяющего всем требованиям метода, который будет также обеспечивать достаточный уровень кибербезопасности на сегменте АСУ ТП.

Итоговая проблема формулируется следующим образом: необходимо обнаружить такие характеристики трафика, передаваемого в промышленных сетях, которые позволят разделить нормальное и аномальное поведение системы без глубокого исследования передаваемых сетевых пакетов, а также позволяет системе сохранять своё быстродействие на том уровне, который является достаточным по требованиям МЭК 61850.

Программируемый логический контроллер (ПЛК) - это вычислительное устройство, осуществляющее обработку данных по принципу «ответ по запросу». Основной характеристикой процесса передачи таких данных является значение длины передаваемого блока и частота передачи [9]. Во-первых, очень важно отметить, что процесс обработки данных является циклическим: ПЛК представляет собой всего лишь небольшой объект большой АСУ ТП, его задачей является выполнение единственной либо небольшого набора задач. Следовательно, обработка данных может быть представлена в виде функции над входными данными, которая возвращает интенсивность передачи данных и длину пакета в качестве результата. Длина переданных данных не зависит от содержимого, переданного в этих данных однако для устройств, выполняющих малое количество задач, этот признак может являться показательным [10].

Вторая важная характеристика ПЛК - это производительность, которая измеряется в количестве запросов за единицу времени и времени ответа на них со стороны сервера. Например, ПЛК компании Siemens – Simatic S7-300 генерирует 1 пакет каждые 150 миллисекунд, ответ со стороны сервера зависит от самого SCADA-сервера, а также средств коммутации, использованных для построения инженерной сети [11].

Используя оба этих параметров, возможно автоматически определять, в каком состоянии находится ПЛК и на каком этапе внутреннего цикла он находится. Внутренний цикл ПЛК представляет собой набор инструкций, которые ПЛК будет выполнять бесконечно до тех пор, пока SCADA-сервер не скажет прекратить или не обновит набор инструкций для исполнения. Алгоритм Брауна [12], основанный на методе экспоненциального скользящего среднего, может быть использован для обучения на результатах работы ПЛК в течение продолжительного периода времени. В этот период обязательно должен быть включен минимум один полный цикл работы для сбора всех состояний, возможных для ПЛК с различными входными параметрами и способами перехода в состояния. Это позволит построить профиль активности ПЛК. Алгоритм позволяет сравнить некоторое представление пакета, полученного в режиме реального времени, с обученными данными и выявить аномалию в том случае, если представление пакета не может быть найдено либо уходит слишком далеко в перспективе.

С использованием алгоритмов машинного обучения необходимо получить представление любого из состояний системы в определенный момент времени как одно из трех состояний системы на основе ключевых характеристик ПЛК: количественных характеристик пакета и производительности [13].

Возможные состояния системы:

- нормальная работа системы;
- состояние, не характерное для нормальной работы системы, однако не нарушающее ее работоспособность;
- состояние, близкое к состоянию сбоя и/или отказа.

Описание предлагаемого метода

Для проверки возможности выявления аномалий в трафике, собранном с маршрутизатора в реальной индустриальной промышленной сети, был использован метод кластеризации «k-средних» [14]. Алгоритм разбивает множество элементов векторного пространства на заранее известное число кластеров. В исследуемом случае число кластеров равно трем:

- кластер с трафиком, характерным для нормальной работы стенда;
- кластер с трафиком, содержащим вектор атаки;
- кластер с трафиком, характеризующим состояние стенда, близкое к состоянию сбоя и/или отказа.

Для кластеризации трафика были выделены следующие характеристики трафика [15]:

- размер исходящего потока (в байтах);
- размер входящего потока (в байтах);
- размер исходящего потока (в пакетах);
- размер входящего потока (в пакетах);
- математическое ожидание размера выходного пакета;
- математическое ожидание размера входного пакета;
- дисперсия размера выходного пакета;
- дисперсия размера входного пакета;
- математическое ожидание времени отправки пакета;
- математическое ожидание времени получения пакета;
- дисперсия времени отправки пакета;
- дисперсия времени получения пакета.

Для набора трафика была получена оценка количества кластеров, результаты оценки предоставлены на рис. 1. Практическая оценка совпадает с ожидаемой:

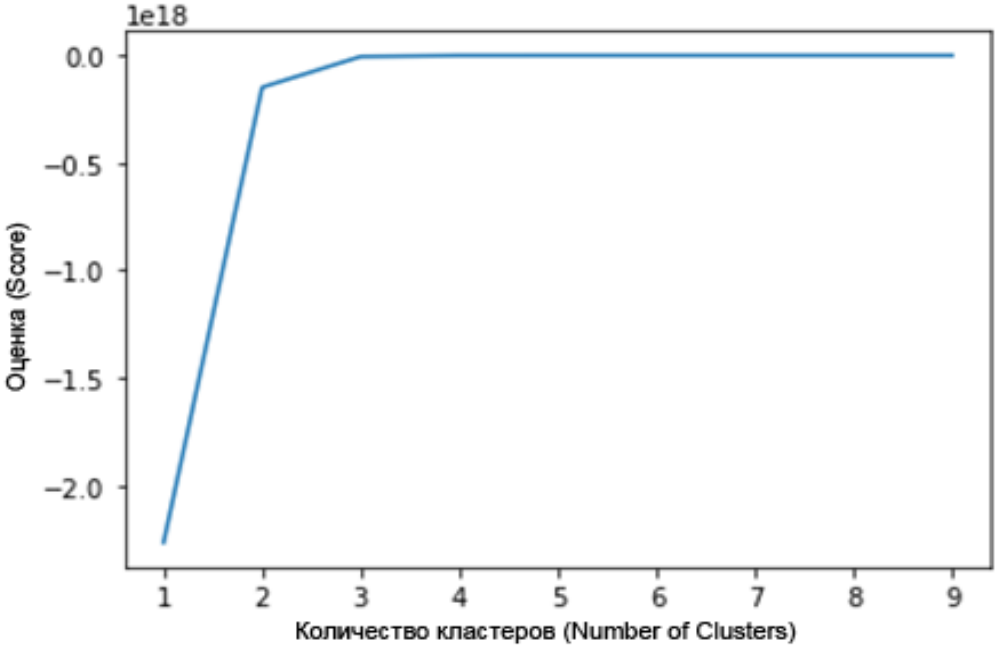

Рис. 1. Оценка количества кластеров алгоритмом k-means
(Fig. 1. Clusters amount estimation via k-means algorithm)

Построение графиков по длинам пакетов в байтах с учетом кластеризации показало результаты, совпадающие с ожидаемыми (рис. 2). Синим цветом обозначены пакеты, характерные для нормальной работы системы. Зеленым – состояния перехода системы. Желтым – состояния отказа. Легко заметить, что кластер переходных состояний находится рядом с нормальным состоянием системы, однако отличается от него. Состояния отказа хаотичны и поэтому оказались расположены далеко от нормальных состояний.

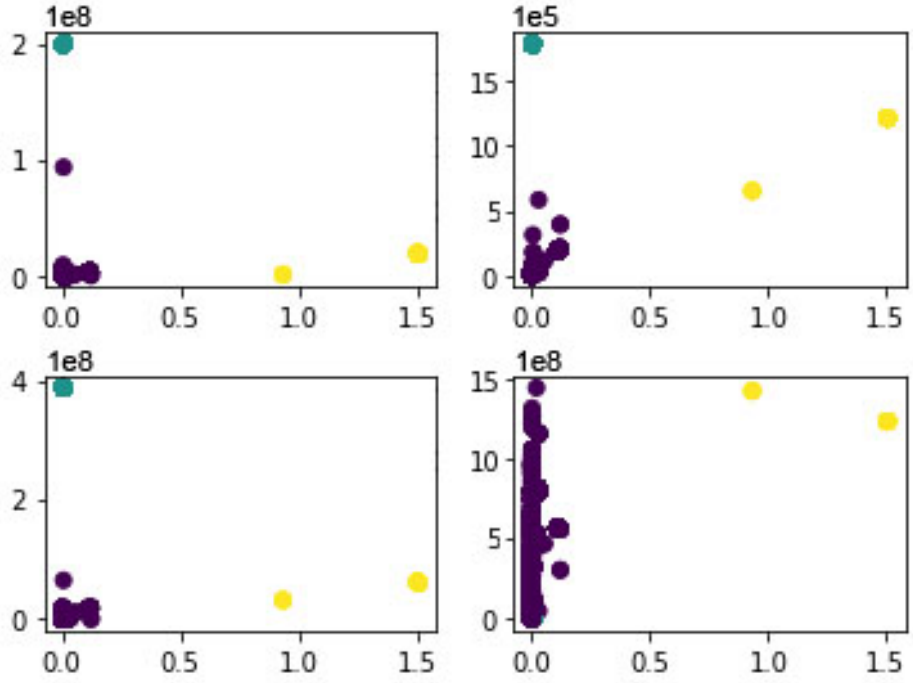

Рис. 2. Результат разбиения трафика на кластеры по четырем различным характеристикам размеров потоков
(Fig. 2. Result of traffic segmentation to clusters using four various specifications of flow sizes)

Построение графиков по числу пакетов в течение одной полной сессии также показало приемлемые результаты (рис. 3):

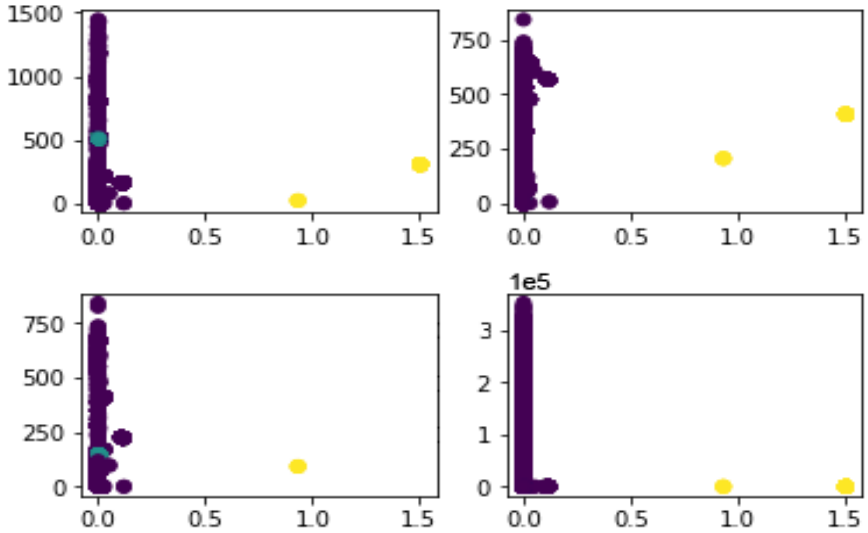

Рис. 3. Результат разбиения трафика на кластеры по четырем различным характеристикам размеров пакетов
(Fig. 3. Result of traffic segmentation to clusters using four various specifications of packet sizes)

Построение графиков по математическому ожиданию времени отправки/получения потока не даёт четкого выделения критических состояний (рис. 4):

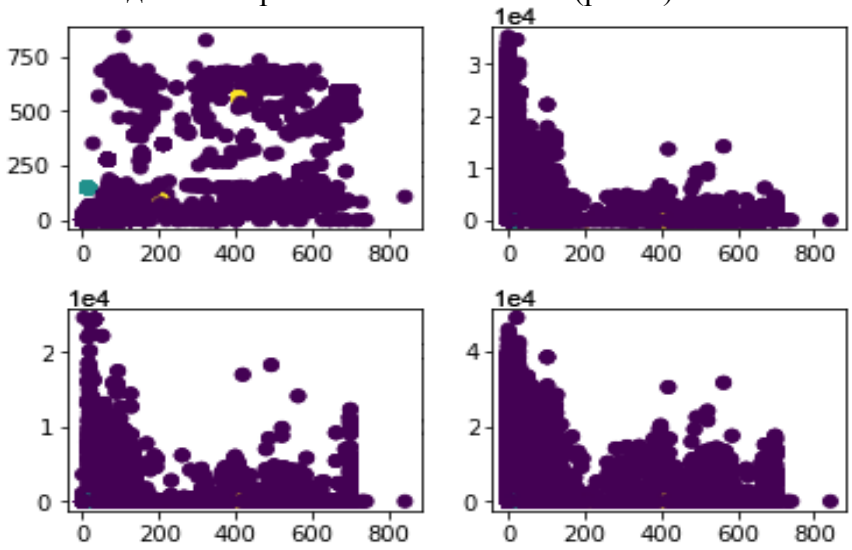

Рис. 4. Результат разбиения трафика на кластеры по четырем временным характеристикам потоков
(Fig. 4. Result of traffic segmentation to clusters using four temporal characteristics of flows)

Построение графиков по временным характеристикам пакетов также не эффективно (рис. 5).

Для проверки согласования исходных выборочных данных с выдвинутой гипотезой, относительно наиболее точно описывающих систему характеристик трафика, были проверены статистические гипотезы первого и второго рода. В качестве проверяемых характеристик были выбраны те, которые показали хорошие результаты на графиках: размеры потоков в байтах и количестве пакетов на входе и выходе узла отдельно. Для вычисления значения ошибок было осуществлено обучение на предварительно исследованных данных, где для каждого состояния была указана принадлежность к каждому кластеру. Для каждого случая, когда верное состояние было воспринято как аномальное, а также аномальное состояние – как верное, осуществлялся инкремент значения соответствующего счетчика.

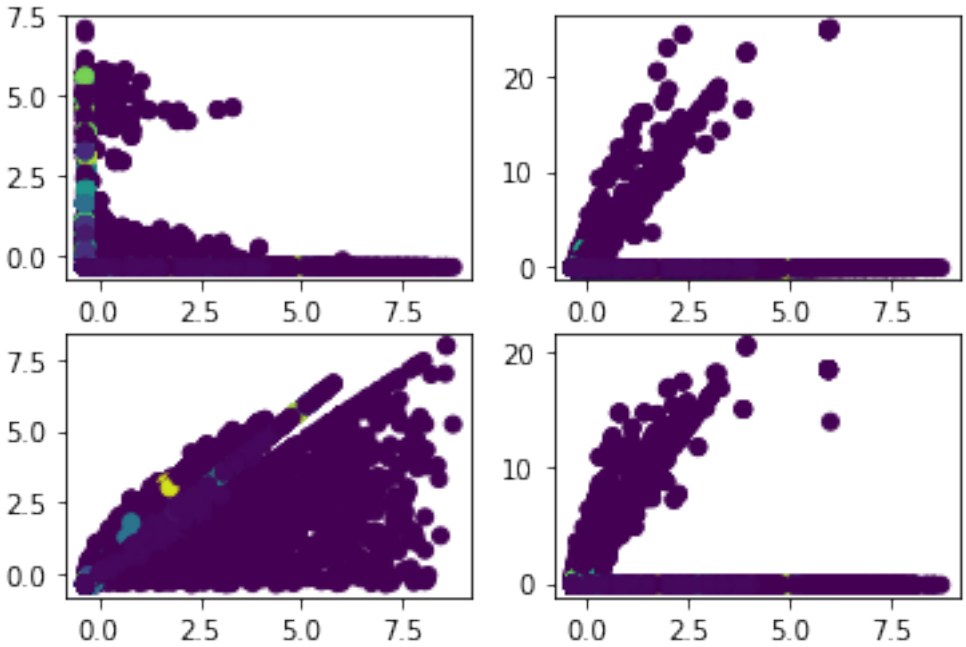

Рис. 5. Результат разбиения трафика на кластеры по четырем временным характеристикам пакетов
(Fig. 5. Result of traffic segmentation to clusters using four temporal characteristics of packets)

Для вычисления значения ошибок первого и второго рода использовалось частное значений счетчиков и общего количества учтенных состояний. Целью вычисления ошибок было уточнить, какая из характеристик даёт более точный результат, однако для предоставленной выборки значения ошибок оказались примерно равны.

Таблица 1. Оценки точности использования методов на основе предложенных характеристик

Характеристика	Ошибка первого рода	Ошибка второго рода
размер исходящего потока (в байтах)	7.70%	7.40%
размер входящего потока (в байтах)	5.34%	5.31%
размер исходящего потока (в пакетах)	7.52%	7.61%
размер входящего потока (в пакетах)	5.36%	5.42%

Заключение

В работе рассматривался подход к получению представления любого из состояний системы в определенный момент времени как одно из трех состояний системы, на основе ключевых характеристик ПЛК: количественных характеристик пакета и производительности. Предлагаемый подход позволил выявить критические состояния на основе анализа сетевого трафика с целью предотвращения возможности появления аномалий во всей системе и помочь оператору индустриальных систем минимизировать ущерб, который мог быть вызван отказом системы. В процессе выделения характеристик промышленного трафика, на основе которых выявление состояний системы в различные моменты времени при помощи алгоритмов кластеризации наиболее эффективно, были получены следующие результаты: наибольшую значимость для промышленного трафика имеют длина входящего и исходящего потока данных в байтах и количество пакетов. Полученные значения ошибок первого и второго рода могут быть использованы для выявления причины ошибок и уточнения предлагаемого метода, а также, с

использованием большего количества данных для обучения, для проведения кросс-валидации и отсеивания избыточных характеристик, что на текущем объеме данных провести невозможно.

СПИСОК ЛИТЕРАТУРЫ:

1. Riis, T. S. (2016). Modeling water distribution systems-integration between SCADA systems and hydraulic network simulation models. Master's thesis, NTNU. [Электронный ресурс] Режим доступа: https://brage.bibsys.no/xmlui/handle/11250/2433613 (дата обращения 26.06.2018).
2. Liu G., Yang Z., Jiang W. (2012) A Method of Remote Interactive Control in Electricity SCADA System Based on Internet. In: Jin D., Lin S. (eds) Advances in Mechanical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 177. Springer, Berlin, Heidelberg. [Электронный ресурс] Режим доступа: https://link.springer.com/chapter/10.1007/978-3-642-31516-9_80 (дата обращения 26.06.2018).
3. R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES, 2006, pp. 623–630. [Электронный ресурс] Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.4368&rep=rep1&type=pdf (дата обращения 26.06.2018).
4. Modbus TCP/IP. [Электронный ресурс] Режим доступа: http://www.simplymodbus.ca/TCP.html (дата обращения 26.06.2018).
5. Kleinmann, A., Wool, A.: Accurate modeling of the siemens S7 SCADA protocol for intrusion detection and digital forensic. JDFSL 9(2), 37–50 (2014). [Электронный ресурс] Режим доступа: http://ojs.jdfsl.org/index.php/jdfsl/article/view/262 (дата обращения 26.06.2018).
6. Dehalwar V., Kalam A., Kolhe M.L., Zayegh A., Dubey A.K. (2018) Integration of IEC 61850 MMS and IEEE 802.22 for Smart Grid Communication. In: Perez G., Mishra K., Tiwari S., Trivedi M. (eds) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 3. Springer, Singapore [Электронный ресурс] Режим доступа: https://link.springer.com/chapter/10.1007/978-981-10-4585-1_7 (дата обращения 26.06.2018).
7. Carcano A., Fovino I.N., Masera M., Trombetta A. (2010) State-Based Network Intrusion Detection Systems for SCADA Protocols: A Proof of Concept. In: Rome E., Bloomfield R. (eds) Critical Information Infrastructures Security. CRITIS 2009. Lecture Notes in Computer Science, vol 6027. Springer, Berlin, Heidelberg. [Электронный ресурс] Режим доступа: https://link.springer.com/chapter/10.1007/978-3-642-14379-3_12 (дата обращения 26.06.2018).
8. Shaji, R.S., Sachin Dev, V. & Brindha, T. Wireless Netw (2018). [Электронный ресурс] Режим доступа: https://doi.org/10.1007/s11276-018-1724-1 (дата обращения 26.06.2018).
9. Rodofile N.R., Schmidt T., Sherry S.T., Djamaludin C., Radke K., Foo E. (2017) Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure. In: Pieprzyk J., Suriadi S. (eds) Information Security and Privacy. ACISP 2017. Lecture Notes in Computer Science, vol 10343. Springer, Cham. [Электронный ресурс] Режим доступа: https://link.springer.com/chapter/10.1007/978-3-319-59870-3_30 (дата обращения 26.06.2018).
10. P. Kiedrowski, "Errors nature of the narrowband plc transmission in smart lighting LV network," International Journal of Distributed Sensor Networks, vol. 2016, Article ID 9592679, 9 pages, 2016. [Электронный ресурс] Режим доступа: http://journals.sagepub.com/doi/full/10.1155/2016/9592679 (дата обращения: 26.06.2018)
11. Tomasz Andrysiak, Łukasz Saganowski, and Piotr Kiedrowski "Anomaly Detection in Smart Metering Infrastructure with the Use of Time Series Analysis", Journal of Sensors Volume 2017 (2017), Article ID 8782131, 15 pages. [Электронный ресурс] Режим доступа: http://journals.sagepub.com/doi/full/10.1155/2016/9592679 (дата обращения 26.06.2018).
12. P. Galeano, D. Pea, and R.S. Tsay,Outlier detection in multivariate time series via projection pursuit. Statistics and econometrics working articles Departamento de Estadistica y Econometrica, Universidad Carlos III, 2004. [Электронный ресурс] Режим доступа: https://pdfs.semanticscholar.org/5c40/b0d6c869dcbd8fd8899f292111a05241488d.pdf (дата обращения 26.06.2018).
13. AlShemeili A., Yeun C.Y., Baek J. (2016) PLC Monitoring and Protection for SCADA Framework. In: Park J., Chao HC., Arabnia H., Yen N. (eds) Advanced Multimedia and Ubiquitous Engineering. Lecture Notes in Electrical Engineering, vol 354. Springer, Berlin, Heidelberg [Электронный ресурс] Режим доступа: https://www.researchgate.net/publication/285449625_PLC_monitoring_and_protection_for_SCADA_framework (дата обращения 26.06.2018).
14. Vávra J., Hromada M. (2017) Determination of Optimal Cluster Number in Connection to SCADA. In: Silhavy R., Silhavy P., Prokopova Z., Senkerik R., Kominkova Oplatkova Z. (eds) Software Engineering Trends and Techniques in Intelligent Systems. CSOC 2017. Advances in Intelligent Systems and Computing, vol 575. Springer, Cham [Электронный ресурс] Режим доступа: https://link.springer.com/chapter/10.1007/978-3-319-57141-6_15 (дата обращения 26.06.2018).
15. Yıldırım N., Uzunoğlu B. (2016) Data Mining via Association Rules for Power Ramps Detected by Clustering or Optimization. In: Gavrilova M., Tan C., Sourin A. (eds) Transactions on Computational Science XXVIII.

Lecture Notes in Computer Science, vol 9590. Springer, Berlin, Heidelberg. [Электронный ресурс] Режим доступа: https://link.springer.com/chapter/10.1007/978-3-662-53090-0_9 (дата обращения 26.06.2018).

REFERENCES:

[1] Riis, T. S. (2016). Modeling water distribution systems-integration between SCADA systems and hydraulic network simulation models. Master's thesis, NTNU. https://brage.bibsys.no/xmlui/handle/11250/2433613 (access date 26.06.2018).

[2] Liu G., Yang Z., Jiang W. (2012) A Method of Remote Interactive Control in Electricity SCADA System Based on Internet. In: Jin D., Lin S. (eds) Advances in Mechanical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 177. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-31516-9_80 (access date 26.06.2018).

[3] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in Power Systems Conference and Exposition, 2006. PSCE '06. 2006 IEEE PES, 2006, pp. 623–630. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.4368&rep=rep1&type=pdf (access date 26.06.2018).

[4] Modbus TCP/IP. http://www.simplymodbus.ca/TCP.html (access date 26.06.2018).

[5] Kleinmann, A., Wool, A.: Accurate modeling of the siemens S7 SCADA protocol for intrusion detection and digital forensic. JDFSL 9(2), 37–50 (2014). http://ojs.jdfsl.org/index.php/jdfsl/article/view/262 (access date 26.06.2018).

[6] Dehalwar V., Kalam A., Kolhe M.L., Zayegh A., Dubey A.K. (2018) Integration of IEC 61850 MMS and IEEE 802.22 for Smart Grid Communication. In: Perez G., Mishra K., Tiwari S., Trivedi M. (eds) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 3. Springer, Singapore. https://link.springer.com/chapter/10.1007/978-981-10-4585-1_7 (access date 26.06.2018).

[7] Carcano A., Fovino I.N., Masera M., Trombetta A. (2010) State-Based Network Intrusion Detection Systems for SCADA Protocols: A Proof of Concept. In: Rome E., Bloomfield R. (eds) Critical Information Infrastructures Security. CRITIS 2009. Lecture Notes in Computer Science, vol 6027. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-14379-3_12 (access date 26.06.2018).

[8] Shaji, R.S., Sachin Dev, V. & Brindha, T. Wireless Netw (2018). https://doi.org/10.1007/s11276-018-1724-1 (access date 26.06.2018).

[9] Rodofile N.R., Schmidt T., Sherry S.T., Djamaludin C., Radke K., Foo E. (2017) Process Control Cyber-Attacks and Labelled Datasets on S7Comm Critical Infrastructure. In: Pieprzyk J., Suriadi S. (eds) Information Security and Privacy. ACISP 2017. Lecture Notes in Computer Science, vol 10343. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-59870-3_30 (access date 26.06.2018).

[10] P. Kiedrowski, "Errors nature of the narrowband plc transmission in smart lighting LV network," International Journal of Distributed Sensor Networks, vol. 2016, Article ID 9592679, 9 pages, 2016. http://journals.sagepub.com/doi/full/10.1155/2016/9592679 (access date: 26.06.2018)

[11] Tomasz Andrysiak, Łukasz Saganowski, and Piotr Kiedrowski "Anomaly Detection in Smart Metering Infrastructure with the Use of Time Series Analysis", Journal of Sensors Volume 2017 (2017), Article ID 8782131, 15 pages. http://journals.sagepub.com/doi/full/10.1155/2016/9592679 (access date 26.06.2018).

[12] P. Galeano, D. Pea, and R.S. Tsay, Outlier detection in multivariate time series via projection pursuit. Statistics and econometrics working articles Departamento de Estadistica y Econometrica, Universidad Carlos III, 2004. https://pdfs.semanticscholar.org/5c40/b0d6c869dcbd8fd8899f292111a05241488d.pdf (access date 26.06.2018).

[13] AlShemeili A., Yeun C.Y., Baek J. (2016) PLC Monitoring and Protection for SCADA Framework. In: Park J., Chao HC., Arabnia H., Yen N. (eds) Advanced Multimedia and Ubiquitous Engineering. Lecture Notes in Electrical Engineering, vol 354. Springer, Berlin, Heidelberg. https://www.researchgate.net/publication/285449625_PLC_monitoring_and_protection_for_SCADA_framework (access date 26.06.2018).

[14] Vávra J., Hromada M. (2017) Determination of Optimal Cluster Number in Connection to SCADA. In: Silhavy R., Silhavy P., Prokopova Z., Senkerik R., Kominkova Oplatkova Z. (eds) Software Engineering Trends and Techniques in Intelligent Systems. CSOC 2017. Advances in Intelligent Systems and Computing, vol 575. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-57141-6_15 (access date 26.06.2018).

[15] Yıldırım N., Uzunoğlu B. (2016) Data Mining via Association Rules for Power Ramps Detected by Clustering or Optimization. In: Gavrilova M., Tan C., Sourin A. (eds) Transactions on Computational Science XXVIII. Lecture Notes in Computer Science, vol 9590. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-662-53090-0_9 (access date 26.06.2018).

Поступила в редакцию – 08 мая 2018 г. Окончательный вариант – 23 августа 2018 г.
Received – May 08, 2018. The final version – August 23, 2018.