УДК 004.056.5
doi:10.31799/1684-8853-2020-4-50-60

Научные статьи
Articles

Метод обнаружения DoS-атак на прикладном уровне в сетях «издатель-подписчик»

Д. И. Дикий[a], *аспирант, orcid.org/0000-0002-8819-8423, dimandikiy@mail.ru*
[a]*Университет ИТМО, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ*

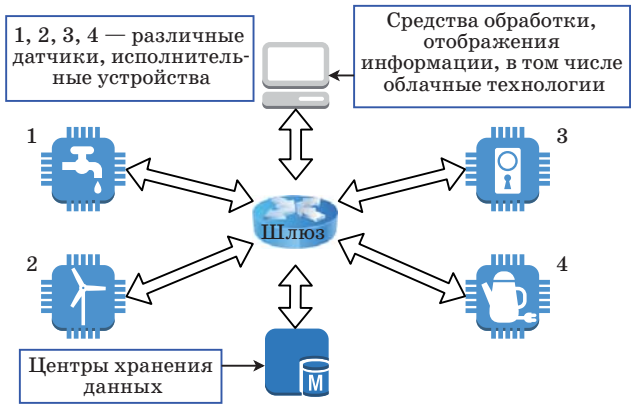
Введение: *для развития киберфизических систем разрабатываются новые технологии и протоколы передачи данных, которые призваны сократить энергетические затраты устройств на коммуникацию. Одним из современных подходов передачи данных для киберфизических систем является модель «издатель-подписчик», которая подвержена угрозе реализации атаки типа «отказ в обслуживании».* ***Цель:*** *разработка модели детектирования атаки типа «отказ в обслуживании», реализуемой на прикладном уровне сетей вида «издатель-подписчик», на основе анализа трафика методами машинного обучения.* ***Результаты:*** *разработана модель средства обнаружения атаки типа «отказ в обслуживании», учитывающая три вида сообщений: подключение, подписку, публикацию. Такой подход позволяет точнее идентифицировать источник атаки, которым может выступать узел сети, конкретное устройство или учетная запись пользователя. В качестве классификаторов были рассмотрены многослойный перцептрон, алгоритм «случайный лес» и метод опорных векторов различных конфигураций. Сгенерированы обучающие и тестовые наборы данных по предложенному вектору признаков. Оценка качества классификации производилась путем расчета F1-меры, коэффициента корреляции Метьюса и точности. Лучшие показатели по всем метрикам принадлежат модели многослойного перцептрона и методу опорных векторов с полиномиальным ядром и методом оптимизации Sequential Minimal Optimization. Однако для последнего метода характерно незначительное снижение качества классификации при ширине окна анализа трафика, близкой к максимальному периоду отправки легальных сообщений обучающего набора данных.* ***Практическая значимость:*** *результаты исследования могут быть использованы для проектирования средств обнаружения вторжений киберфизических систем, использующих модель «издатель-подписчик», а также иных систем, построенных на этом подходе.*

Ключевые слова *— DoS-атаки, «издатель-подписчик», машинное обучение, метод опорных векторов, «случайный лес», искусственная нейронная сеть.*

Для цитирования: Дикий Д. И. Метод обнаружения DoS-атак на прикладном уровне в сетях «издатель-подписчик». *Информационно-управляющие системы*, 2020, № 4, с. 50–60. doi:10.31799/1684-8853-2020-4-50-60
For citation: Dikii D. I. DoS attack detection at application level in publish-subscribe networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 4, pp. 50–60 (In Russian). doi:10.31799/1684-8853-2020-4-50-60

Введение

В настоящее время огромное внимание уделяется киберфизическим системам (КФС) [1] и их частным реализациям в виде умного города, умного дома, интернета вещей, которые позволяют автоматизировать производственные, бытовые и другие процессы. Одним из подходов, который используется для организации межмашинной коммуникации в КФС, является модель передачи данных «издатель-подписчик» [2]. Данная модель позволяет организовать передачу показателей датчиков и данных исполнительных устройств одновременно целой группе получателей. Модель «издатель-подписчик» реализована в таких протоколах, как AMQP, MQTT, XMPP и др. Существует два варианта организации сетевого взаимодействия по этой модели: распределенный и основанный на использовании шлюза. Второй вариант (рис. 1) наиболее распространен в небольших вычислительных сетях и строится по топологии «звезда». Он обладает простотой в развертывании и масштабируемости, легок в администрировании. При этом весь трафик проходит через шлюз, который отвечает за адресацию и логистику сообщений. Наряду со множеством преимуществ, которые предоставляет модель «издатель-подписчик», появляются новые угрозы информационной безопасности, свойственные именно этой модели, например, несанкционированный доступ к информации из-за



■ ***Рис. 1.*** Структура сети КФС по модели «издатель-подписчик», использующей шлюз
■ ***Fig. 1.*** CPS network structure according to the publish-subscribe model using a gateway

отсутствия разграничения доступа к ней на шлюзе, атаки типа «отказ в обслуживании», сканирование сети на наличие открытых портов и хостов, угрозы неавторизованного доступа к шлюзу.

Защита информации в КФС является актуальной задачей. Эти системы способствовали развитию новых технологий, которые должны обеспечивать надежную коммуникацию между устройствами на больших расстояниях, например, технологии LoRa, XNB и др. Кроме разработок на физическом уровне, создаются протоколы передачи данных поверх уже существующих сетей, например, протоколы прикладного уровня CoAP, MQTT. Одним из главных требований к этим протоколам является уменьшение размера служебных заголовков. Это требование основано на том, что многие устройства КФС обладают автономным ограниченным источником питания. Сокращение объемов передаваемой информации позволяет увеличить продолжительность использования этих устройств.

Одной из наиболее актуальных угроз КФС является возможность реализации атаки типа «отказ в обслуживании». Этот вид атаки может быть реализован на физическом, а также на сетевом и прикладном уровнях. Если рассматривать беспроводные сенсорные сети как элемент КФС, то для них характерны атаки типа «отказ в обслуживании» в виде зашумления радиосигнала — jamming attack [3, 4]. Помещая источник сильного шума вблизи приемников и передатчиков, можно добиться нарушения передачи данных [5]. Другой вид атак, также вызывающий отказ в обслуживании, характерен для КФС в виде одноранговых сетей — атака Сивиллы [6]. Также для КФС типичны атаки, заключающиеся в злонамеренном истощении элементов автономного питания устройства [7]. Реализация этой атаки приведет к временной неработоспособности устройства и затратам на замену элемента питания. Атаки типа «отказ в обслуживании» используются как инструмент деструктивного воздействия в ботнет-сетях [8].

В отличие от стандартных методов реализации атаки типа «отказ в обслуживании» на сетевом уровне по протоколам TCP/IP, сеть, построенная на модели «издатель-подписчик», может быть выведена из строя путем атаки на прикладном уровне [9–11]. Так как шлюз является узким местом сети, то чаще всего именно он становится целью атаки. Суть атаки сводится к генерации большого числа запросов таким образом, чтобы шлюз не справился с нагрузкой. Следовательно, разработка методов детектирования этого вида атак на прикладном уровне является актуальной задачей.

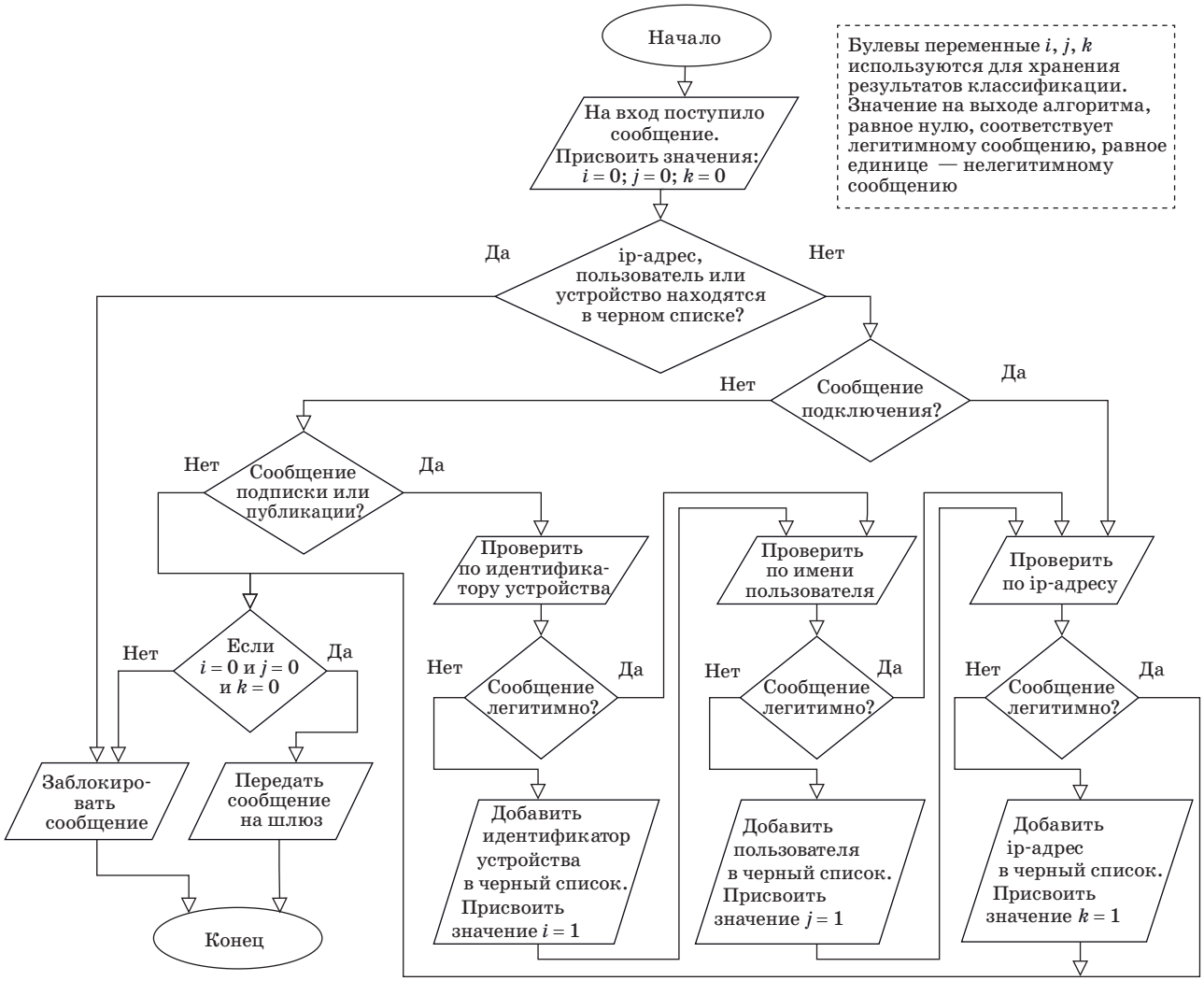
Цель исследования состоит в разработке модели средства детектирования атаки типа «отказ в обслуживании», реализуемой на прикладном уровне сетей вида «издатель-подписчик», на основе анализа трафика методами машинного обучения. В качестве объекта исследования в данной работе рассмотрен протокол MQTT, который реализует исследуемую модель межмашинной коммуникации. В отличие от большинства других протоколов, модель «издатель-подписчик» в протоколе MQTT является основной, а не расширяет уже имеющийся функционал в рамках протокола.

Возможности протокола MQTT как инструмента генерации большого числа запросов в рамках атаки типа «отказ в обслуживании» были рассмотрены во многих работах. Например, в работе [12] предложен метод, основанный на нечеткой логике, который детектирует атаки, производимые с помощью сообщений подключения к шлюзу. В этом исследовании удалось добиться точности классификации 0,909. Протокол MQTT поддерживает три уровня качества обслуживания (Quality of Service — QoS). В зависимости от выбранного уровня QoS изменяется количество служебных сообщений, участвующих в передаче информации. Следовательно, появляется возможность оптимизировать нагрузку на сеть, изменяя уровень QoS [13]. Аналогичный подход к защите от атак сводится к оптимизации загрузки шлюза на основе показаний использования вычислительных ресурсов его центрального процессора [14]. Ограничение частоты сообщений может значительно снизить риск реализации угрозы [15]. Для обнаружения сетевой аномалии недостаточно учитывать только частоту сообщений и уровень QoS. Другими важными параметрами являются криптографические преобразования, значительно влияющие на время обработки сообщения и, следовательно, на загруженность шлюза. Большое значение имеет размер полезной нагрузки. Чем больше полезная нагрузка, тем больше временных и вычислительных ресурсов потребуется на шлюзе [16].

Алгоритм детектирования атаки

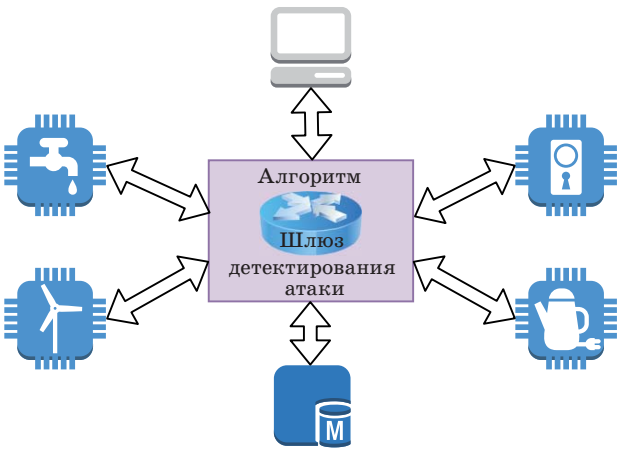
Модель «издатель-подписчик» предполагает три ключевые фазы коммуникации: подключение к шлюзу, подписку на тему, публикацию сообщения на тему. В протоколе MQTT эти три фазы реализованы посредством трех типов сообщений: connect, subscribe, publish [17]. Аналогичные механизмы предусмотрены и в других протоколах «издатель-подписчик». Эти три вида сообщений будут использованы для анализа сетевого трафика. Кроме того, как показано в работе [9], злоупотребление любым из этих трех видов сообщений способно вызвать нестабильную работу шлюза.

Отправителя сообщения можно идентифицировать несколькими способами. Сообщения под-



■ ***Рис. 2.*** Алгоритм анализа трафика в сети «издатель-подписчик»
■ ***Fig. 2.*** Algorithm of traffic analysis in the publish-subscribe network

ключения к шлюзу не требуют авторизации на шлюзе и могут быть отправлены любым устройством, которое знает адрес и порт шлюза и имеет доступ к сети. В таком случае отправителя можно идентифицировать только по его сетевому адресу. Имя пользователя и идентификатор устройства, указываемые в теле сообщения подключения, могут быть любыми, в том числе несуществующими. Сообщения подписки и публикации обрабатываются только от авторизованных на шлюзе устройств. Отправителя этих сообщений можно идентифицировать по сетевому адресу, имени пользователя и уникальному идентификатору устройства. Таким образом, в разработанном алгоритме детектирования атаки (рис. 2) применяется либо один, либо три классификатора в зависимости от вида анализируемого сообщения. Булевы переменные i, j, k используются для хранения результатов классификации по



■ ***Рис. 3.*** Схема расположения средства защиты от атаки типа «отказ в обслуживании», реализующего предлагаемый алгоритм
■ ***Fig. 3.*** Scheme of the denial-of-service attack protection that implements the proposed algorithm

идентификатору устройства, имени пользователя и ip-адресу соответственно. Значение этих переменных на выходе алгоритма, равное нулю, соответствует легитимному сообщению, равное единице — нелегитимному сообщению.

Средство обнаружения атаки типа «отказ в обслуживании», реализующее предлагаемый алгоритм, следует располагать на входе шлюза таким образом, чтобы все входящие сообщения сперва обрабатывались классификаторами и уже затем шлюзом (рис. 3).

Методы и оценка качества классификации

Классификация сетевого трафика на аномальный и легитимный часто осуществляется методами машинного обучения. Большинство работ по детектированию атаки типа «отказ в обслуживании» посвящены анализу трафика по TCP-протоколу. К самым распространенным методам относятся алгоритм k-ближайших соседей, наивный байесовский классификатор, метод опорных векторов, искусственные нейронные сети (ИНС), деревья решений и некоторые другие [18–21]. В данном исследовании в качестве классификаторов рассмотрены метод опорных векторов, ИНС, алгоритм «случайный лес». Выбор этих методов определяется тем, что они показали свою высокую эффективность при решении аналогичных задач на сетевом уровне.

Метод опорных векторов основан на построении оптимальной гиперплоскости в многомерном пространстве, разделяющей объекты различных классов. Этот подход был использован для детектирования атак в работах [22, 23] и показал отличные результаты. На форму гиперплоскости огромное влияние оказывает функция ядра. Наиболее распространенными функциями ядра являются линейная, полиномиальная, радиально-базисная, представленные следующими уравнениями соответственно:

$$K(x_i, x_j) = x_i^{\mathrm{T}} x_j; \quad (1)$$

$$K(x_i, x_j) = (x_i^{\mathrm{T}} x_j + c)^k; \quad (2)$$

$$K(x_i, x_j) = \exp(\gamma \|x_i - x_j\|^2), \quad (3)$$

где x_i и x_j — элементы классифицируемого множества; c, γ — константы; k — степень полинома.

При использовании метода опорных векторов применяются различные методы оптимизации, например метод SMO (Sequential Minimal Optimization) [24].

Искусственные нейронные сети нашли широкое применение в решении задач распознавания образов, в том числе и детектирования атаки типа «отказ в обслуживании». Например, в работе [25] точность ИНС составила порядка 0,99. Моделей ИНС существует довольно большое количество: это и обычный многослойный перцептрон Ф. Розенблатта, и рекуррентные ИНС, и ИНС с краткосрочной памятью (LSTM), и др. Основой ИНС является нейрон с соответствующей функцией активации. Наиболее часто в задачах распознавания образов используют сигмоидальную функцию активации нейрона

$$F(x) = 1/(1 + e^{(-x)}), \quad (4)$$

где x — это сумма произведений выходных сигналов нейронов предыдущего слоя на соответствующий весовой коэффициент.

Обучение ИНС производится, как правило, алгоритмом обратного распространения ошибки либо генетическим алгоритмом.

Класс алгоритмов, основанный на деревьях решений, также применяется для детектирования атаки типа «отказ в обслуживании» [26]. Идея алгоритма дерева решений сводится к построению направленного графа от корня к листьям таким образом, чтобы распределение вероятностей в листьях было равномерным. Классификатор на основе композиции из нескольких деревьев решений, генерируемых методом бутсрепа, получил большое распространение под названием «случайный лес». Оптимизация деревьев решений в рамках алгоритма «случайный лес» производится по оценкам энтропии, индекса Джинни или частоты ошибочных классификаций, представленными следующими уравнениями соответственно:

$$I = -\sum P(w_j)\log_2 P(w_j); \quad (5)$$

$$I = 1 - \sum P^2(w_j); \quad (6)$$

$$I = 1 - \max P(w_j), \quad (7)$$

где $P(w_j)$ — вероятность отнесения объекта w к классу j.

В данной работе в качестве классификаторов будут рассмотрены следующие алгоритмы: ИНС в виде многослойного перцептрона, «случайный лес», метод опорных векторов с линейной и радиально-базисной функциями ядра, метод опорных векторов с методом оптимизации SMO полиномиальной и радиально-базисной функциями ядра.

Для оценки качества классификации рассчитывались точность, F1-мера и коэффициент корреляции Мэтьюса. Значения этих параметров вычисляются исходя из количества правильно и ошибочно классифицированных объектов тестовой выборки:

— точность

$$A = (TP + TN)/(TP + TN + FP + FN); \quad (8)$$

— F1-мера

$$P = TP/(TP + FP); \quad (9)$$

$$R = TP/(TP + FN); \quad (10)$$

$$F = (2 \times P \times R)/(P + R); \quad (11)$$

— коэффициент корреляции Мэтьюса

$$M = (TP \times TN - FP \times FN)/((TP + FN) \times \times (TP + FP) \times (TN + FP) \times (TN + FN))^{1/2}. \quad (12)$$

В формулах (8)–(12) TP соответствует истинно положительным классификациям, TN — истинно отрицательным, FP — ложноположительным, а FN — ложноотрицательным.

Вектор признаков

Для классификации трафика должен быть сформирован вектор признаков с учетом модели «издатель-подписчик». Так как исследуемая модель передачи информации состоит из трех основных фаз: подключения, подписки и публикации, — то для каждой из них должен быть сформирован характерный ей вектор признаков, как представлено в табл. 1.

Основой атаки типа «отказ в обслуживании» является повышенная частота сообщений. Чтобы своевременно обнаружить атаку на начальном ее этапе, необходимо определить оптимальный интервал времени (далее — ширина окна), в течение которого рассчитываются характеристики трафика для дальнейшего анализа. Малые значения ширины окна приведут к росту ложноотрицательных результатов. С другой стороны, большие значения ширины окна отрицательно влияют на быстродействие детектирования. Вторым параметром, также влияющим на загруженность шлюза при обработке сообщений подключения, является среднее значение времени между двумя последовательными сообщениями. Для сообщений подключения важное значение имеет факт использования криптографических преобразований, в том числе процесс генерации общего сессионного ключа между шлюзом и устройством. Как правило, в КФС используется протокол TLS, который требует большого количества вычислительных и временных затрат во время установления защищенного соединения. В качестве идентификатора сообщения может выступать только сетевой адрес устройства.

Вектор признаков сообщения подписки на тему состоит из тех же параметров, что и вектор признаков сообщения подключения к шлюзу. Наличие криптографических преобразований, а это, как правило, симметричное шифрование, незначительно влияет на производительность шлюза. Источник атаки по сообщению подписки на тему можно идентифицировать не только по его сетевому адресу, но и по имени пользователя и идентификатору устройства, так как такие запросы возможно отправлять только с авторизованного устройства.

Для сообщения публикации помимо вышеперечисленных параметров необходимо учитывать размер полезной нагрузки. Чем больше размер нагрузки, тем больше вычислительных операций производится на шлюзе. К тому же на производительность шлюза как ретранслятора сообщений будет оказывать влияние количество подписчиков на тему. В большинстве протоколов модели «издатель-подписчик» для обеспечения гарантированности доставки сообщений используются уровни QoS, что также влияет на нагрузку сети. Этот механизм предусмотрен в таких протоколах, как DDS, MQTT, AMQP.

■ ***Таблица 1***. Вектор признаков трафика модели «издатель-подписчик» в зависимости от вида сообщений
■ ***Table 1***. Traffic feature vector of publish-subscribe model depending on message type

Параметр	Вид сообщения		
	Подключение	Подписка	Публикация
IP-адрес	+	+	+
Имя пользователя	–	+	+
Идентификатор устройства	–	+	+
Частота сообщений	+	+	+
Среднее значение интервала времени между сообщениями	+	+	+
Наличие криптографических преобразований трафика	+	+	+
Уровни качества QoS	–	–	+
Размер полезной нагрузки	–	–	+
Количество подписчиков	–	–	+

Наборы данных

На настоящий момент в открытом доступе отсутствуют наборы данных сетевого трафика по модели «издатель-подписчик», содержащие примеры атаки типа «отказ в обслуживании» на прикладном уровне со всей необходимой для данного исследования информацией. В связи с этим

для обучения и тестирования классификаторов были сгенерированы соответствующие наборы данных. Моделирование трафика производилось с нескольких ЭВМ, на которых были запущены MQTT-клиенты, созданные с помощью библиотеки paho-mqtt [27]. Сбор и анализ данных производился на модифицированном шлюзе Moquette с открытым исходным кодом [28]. В качестве шлюза использовался одноплатный микрокомпьютер Raspberry Pi 3 model B. Алгоритмы классификации использовались из программного пакета WEKA [29]. Основные настраиваемые параметры моделируемых наборов данных представлены в табл. 2.

Для легитимного трафика программным путем задавался максимальный период между сообщениями. Сообщения публикации дополнительно характеризовались количеством подписчиков и размером полезной нагрузки. В рамках исследования было смоделировано по два обучающих и тестовых набора для легитимного трафика. Главным отличием этих наборов данных является различный максимальный период времени между отправкой легальных сообщений, а для сообщений публикации также изменялся размер полезной нагрузки и количество подписчиков. Использование нескольких обучающих наборов данных позволит оценить влияние отличий в этих наборах на результаты классификации.

Набор данных, содержащий аномальный трафик, включал в себя примеры не только частой отправки сообщений, но и примеры со значительно большими размерами нагрузки и количеством получателей для сообщений публикации. Например, трафик сообщений большого размера, но с обычной частотой и количеством получателей.

Тестовый набор данных генерировался аналогичным образом, только с расширенными границами изменяемых параметров: периодичности, размера нагрузки, количества подписчиков. Расширение границ тестовых наборов производилось для того, чтобы оценить способность

■ ***Таблица 2***. Основные задаваемые параметры при генерации наборов данных
■ ***Table 2***. Main changed parameters of dataset generation

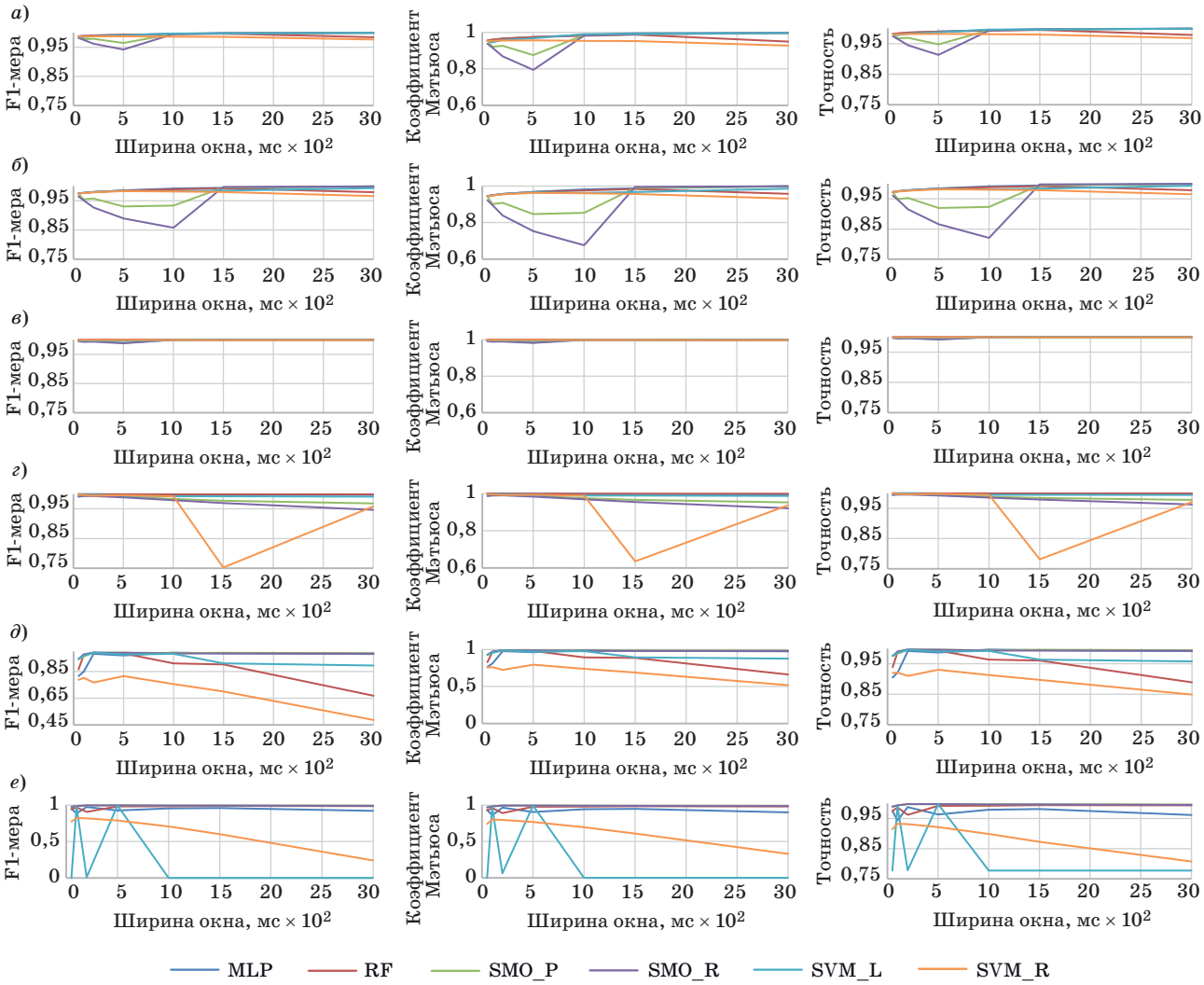
Набор данных	Легитимный трафик, вариант 1	Легитимный трафик, вариант 2	Аномальный трафик
Подключение			
Частота сообщений			
Обучение	Не реже одного сообщения в 500 мс	Не реже одного сообщения в 1000 мс	Максимальная частота
Тестирование	Не реже одного сообщения в 250 мс	Не реже одного сообщения в 500 мс	То же
Подписка			
Частота сообщений			
Обучение	Не реже одного сообщения в 500 мс	Не реже одного сообщения в 5000 мс	Максимальная частота
Тестирование	Не реже одного сообщения в 250 мс	Не реже одного сообщения в 2500 мс	То же
Публикация			
Частота сообщений			
Обучение	Не реже одного сообщения в 500 мс	Не реже одного сообщения в 5000 мс	Максимальная частота
Тестирование	Не реже одного сообщения в 250 мс	Не реже одного сообщения в 2500 мс	То же
Размер полезной нагрузки, байт			
Обучение	1–80	1–800	60 000–80 000
Тестирование	1–120	1–1200	40 000–80 000
Количество подписчиков, ед.			
Обучение	1–5	1–10	50–100
Тестирование	1–8	1–15	35–100

методов машинного обучения классифицировать трафик, явно не относящийся к одному из двух классов согласно обучающим наборам.

Результаты исследования

Для решения задачи поиска оптимального классификатора необходимо определить минимальную ширину окна, при которой результаты классификации достаточно высоки. В данной работе были рассмотрены следующие значения ширины окна: 50, 100, 200, 500, 1000, 1500, 3000 мс. Результаты классификации в виде значений F1-меры, коэффициента корреляции Мэтьюса и точности представлены на рис. 4, где MLP соответствует модели многослойного перцептрона, RF — алгоритму «случайный лес», SMO_P — методу опорных векторов с полиномиальным ядром и оптимизацией SMO, SMO_R — методу опорных векторов с радиально-базисным ядром и оптимизацией SMO, SVM_L — методу опорных векторов с линейным ядром, SVM_R — методу опорных векторов с радиально-базисным ядром.

Все три метрики (точность, F1-мера и коэффициент корреляции Мэтьюса) показывают одинаковую динамику в рамках одного и того же классификатора. Для сообщений подключения результаты всех классификаторов, кроме методов SMO_P и SMO_R, находятся в пределах небольшого диапазона для всех значений ширины окон. При этом стоит отметить, что при использовании



■ ***Рис. 4.*** Значения F1-меры, коэффициента корреляции Мэтьюса и точности классификаций при использовании легитимного трафика первого варианта для сообщений подключения (*а*), подписки (*в*), публикации (*д*); при использовании легитимного трафика второго варианта для сообщений подключения (*б*), подписки (*г*), публикации (*е*)

■ ***Fig. 4.*** The values of F1-score, Matthews correlation coefficient and accuracy of the classifications using the legitimate traffic of the first variant for message type connect (*а*), subscribe (*в*), publish (*д*); using the legitimate traffic samples of the second variant for message type connect (*б*), subscribe (*г*), publish (*е*)

алгоритмов с оптимизацией SMO худшие результаты находятся в области ширины окна, равной максимальному периоду отправки легальных сообщений в обучающем наборе. Таким образом, наибольшее влияние обучающего набора на итоговый результат оказывается при использовании SMO_P и SMO_R.

В случае сообщений подписки все классификаторы показали отличные результаты. Исключение составляет метод SVM_R, который показал один результат, резко контрастирующий на общем фоне. Как и для сообщений подключения, методы SMO_P и SMO_R показывают ухудшение качества классификации в области значений ширины окна, близкой к максимальному периоду отправки легальных сообщений, но в меньших масштабах. Высокие показатели всех классификаторов связаны с тем, что время обработки этого вида сообщений намного меньше, чем у сообщений подключения и публикации.

Наиболее интересная ситуация наблюдается для сообщений публикации. Метод SVM_L не справился с поставленной задачей при нескольких значениях ширины окна на одном наборе данных и показал не самые лучшие результаты на другом. Качество распознавания с помощью метода SVM_R уступает другим алгоритмам. Аналогичная динамика, но с чуть большими значениями метрик, наблюдается у алгоритма «случайный лес».

Таким образом, среди всех рассмотренных алгоритмов можно выделить модель многослойного перцептрона, значение F1-меры которого не опустилось ниже уровня 0,9 при ширине окна более 100 мс на всех исследуемых наборах данных. Динамика алгоритма «случайный лес» зависит от максимального периода отправки легитимных сообщений обучающего набора. При ширине окна меньшей, чем этот период, алгоритм показывает хорошие результаты, но при последующем увеличении ширины окна качество классификации начинает ухудшаться. Алгоритмы SVM_R и SVM_L показали нестабильную работу. Напротив, метод опорных векторов в виде SMO_P и SMO_R показал высокое качество распознавания — значения F1-меры не опускались ниже уровня 0,85. При этом результаты SMO_P лучше, чем у SMO_R.

Заключение

Одной из самых легко реализуемых угроз в исследуемых сетях является атака типа «отказ в обслуживании» на прикладном уровне. Предложен алгоритм детектирования атаки, позволяющий определить ее источник: узел сети, отдельное устройство или учетную запись. В качестве анализаторов трафика были рассмотрены классификаторы на основе методов машинного обучения, из которых наиболее подходящими для детектирования атаки по предлагаемому вектору признаков являются модель многослойного перцептрона при ширине окна более 100 мс и метод опорных векторов с полиномиальным ядром и методом оптимизации SMO. Однако при использовании последнего стоит учитывать локальную особенность снижения качества распознавания при ширине окна, приблизительно равной периоду отправки легальных сообщений в обучающей выборке. Результаты данного исследования будут полезны при проектировании программных и аппаратных средств защиты сетей КФС. В отличие от исследований других научных групп, чьи работы посвящены отдельному виду сообщений модели «издатель-подписчик», данная работа позволяет рассмотреть предлагаемый алгоритм детектирования атаки типа «отказ в обслуживании» как комплексное решение для анализа трафика всех трех видов сообщений. Произведено сравнение применения нескольких методов машинного обучения для решения поставленной задачи. Дальнейшие исследования будут продолжены в области анализа и проектирования систем защиты сетей, реализующих модель «издатель-подписчик» на базе конкретных протоколов с учетом их особенностей.

Финансовая поддержка

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90051.

Financial support

The reported study was funded by RFBR, project number 19-37-90051.

Литература

1. **Lee J., Bagheri B., Kao H.** A Cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 2015, vol. 3, pp. 18–23. doi:10.1016/j.mfglet.2014.12.001
2. **Henneke D., Elattar M., Jasperneite J.** Communication patterns for cyber-physical systems. *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, 2015, pp. 1–4. doi:10.1109/ETFA.2015.7301623
3. **Vadlamani S., Eksioglu B., Medal H., Nandi A.** Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*,

2016, vol. 172, pp. 76–94. doi:10.1016/j.ijpe.2015.11.008
4. **Li Y., Shi L., Cheng P., Chen J., Quevedo D. E.** Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 2015, vol. 60, no. 10, pp. 2831–2836. doi:10.1109/TAC.2015.2461851
5. **Zhang H., Qi Y., Wu J., Fu L., He L.** DoS attack energy management against remote state estimation. *IEEE Transactions on Control of Network Systems*, 2018, vol. 5, no. 1, pp. 383–394. doi:10.1109/TCNS.2016.2614099
6. **Polyzos G. C., Fotiou N.** Building a reliable Internet of things using information-centric networking. *Journal of Reliable Intelligent Environments*, 2015, vol. 1, pp. 47–58. doi:10.1007/s40860-015-0003-5
7. **Desnitsky V. A., Kotenko I. V., Rudavin N. N.** Protection mechanisms against energy depletion attacks in cyber-physical systems. *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Saint-Petersburg and Moscow, Russia, 2019, pp. 214–219. doi:10.1109/EIConRus.2019.8656795
8. **Perrone G., Vecchio M., Pecori R., Giaffreda R.** The day after mirai: A survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices. *The 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS)*, 2017, Porto, Portugal, pp. 246–253. doi:0.5220/0006287302460253
9. **Дикий Д. И.** Анализ протокола MQTT на атаки «отказ в обслуживании». *Научно-технический вестник информационных технологий, механики и оптики*, 2020, т. 20, № 2, с. 185–194. doi:10.17586/2226-1494-2020-20-2-185-194
10. **Chifor B., Patriciu V.** Mitigating DoS attacks in publish-subscribe IoT networks. *The 9th International Conference: Electronics, Computers and Artificial Intelligence (ECAI 2017)*, 2017, pp. 1–6. doi:10.1109/ECAI.2017.8166463
11. **Nebbione G., Calzarossa M.** Security of IoT application layer protocols: challenges and findings. *Future Internet*, 2020, vol. 12, no. 55, pp. 1–20. doi:10.3390/fi12030055
12. **Haripriya A. P., Kulothungan K.** Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *Eurasip Journal on Wireless Communications and Networking*, 2019, vol. 90. doi:10.1186/s13638-019-1402-8
13. **Potrino G., De Rango F., Fazio P.** A Distributed mitigation strategy against DoS attacks in edge computing. *2019 Wireless Telecommunications Symposium (WTS)*, New York City, NY, USA, 2019, pp. 1–7. doi:10.1109/WTS.2019.8715543
14. **Jo H., Jin H.** Adaptive periodic communication over MQTT for large-scale cyber-physical systems. *IEEE 3rd International Conference on Cyber-Physical Systems, Networks, and Applications*, 2015, Hong Kong, pp. 66–69. doi:10.1109/CPSNA.2015.21
15. **Potrino G., De Rango F., Santamaria A. F.** Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker. *IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, Marrakesh, Morocco, 2019, pp. 1–6. doi:10.1109/WCNC.2019.8885553
16. **Firdous S. N., Baig Z., Valli C., Ibrahim A.** Modelling and evaluation of malicious attacks against the IoT MQTT protocol. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Exeter, 2017, pp. 748–755. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115
17. OASIS Standart MQTT Version 3.1.1. OASIS. 2014. 81 p. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.pdf (дата обращения: 04.04.2020).
18. **Gharibian F., Ghorbani A. A.** Comparative study of supervised machine learning techniques for intrusion detection. *The Fifth Annual Conference on Communication Networks and Services Research (CNSR '07)*, 2007, Fredericton, NB, pp. 350–358. doi:10.1109/CNSR.2007.22
19. **Anbar M., Abdullah R., Hasbullah I. H., Chong Y., Elejla O. E.** Comparative performance analysis of classification algorithms for intrusion detection system. *The 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, Auckland, pp. 282–288. doi:10.1109/PST.2016.7906975
20. **Barati M., Abdullah A., Udzir N. I., Mahmod R., Mustapha N.** Distributed denial of service detection using hybrid machine learning technique. *The International Symposium on Biometrics and Security Technologies (ISBAST)*, 2014, Kuala Lumpur, pp. 268–273. doi:10.1109/ISBAST.2014.7013133
21. **Xiao L., Wan X., Lu X., Zhang Y., Wu D.** IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine*, 2018, vol. 35, no. 5, pp. 41–49. doi:10.1109/MSP.2018.2825478
22. **Jianjian D., Yang T., Feiyue Y.** A novel intrusion detection system based on IABRBFSVM for wireless sensor networks. *Procedia Computer Science*, 2018, vol. 131, pp. 1113–1121. doi:10.1016/j.procs.2018.04.275
23. **Abusitta A., Bellaiche M., Dagenais M.** An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. *Journal of Cloud Computing*, 2018, vol. 7, no. 9. doi:10.1186/s13677-018-0109-4
24. **Platt J. C.** Sequential minimal optimization: A fast algorithm for training support vector machines. *Microsoft Research, Technical Report MSR-TR-98-14*, 1998, pp. 1–21.
25. **Hodo E., Bellekens X., Hamilton A., Dubouilh P.-L., Iorkyase E., Tachtatzis C., Atkinson R.** Threat analy-

sis of IoT networks using artificial neural network intrusion detection system. *International Symposium on Networks, Computers and Communications (ISNCC)*, Yasmine Hammamet, 2016, pp. 1–6. doi:10.1109/ISNCC.2016.7746067
26. **Sangkatsanee P., Wattanapongsakorn N., Charnsripinyo C.** Practical real-time intrusion detection using machine learning approaches. *Computer Communications*, 2011, vol. 34, pp. 2227–2235. doi:10.1016/j.comcom.2011.07.001
27. Paho-MQTT library for Python. https://pypi.org/project/paho-mqtt/ (дата обращения: 04.04.2020).
28. Moquette project open source code. https://github.com/moquette-io/moquette (дата обращения: 04.04.2020).
29. WEKA project. https://www.cs.waikato.ac.nz/ml/weka/ (дата обращения: 04.04.2020).

UDC 004.056.5
doi:10.31799/1684-8853-2020-4-50-60

DoS attack detection at application level in publish-subscribe networks

D. I. Dikii[a], Post-Graduate Student, orcid.org/0000-0002-8819-8423, dimandikiy@mail.ru
[a]ITMO University, 49, Kronverkskii Pr., 197101, Saint-Petersburg, Russian Federation

Introduction: For the development of cyberphysical systems, new technologies and data transfer protocols are being developed, in order to reduce the energy costs of communication devices. One of the modern approaches to data transmission in cyberphysical systems is the publish-subscribe model, which is subject to a denial-of-service attack. **Purpose:** Development of a model for detecting a DoS attack implemented at the application level of publish-subscribe networks based on the analysis of their traffic using machine learning methods. **Results:** A model is developed for detecting a DoS attack, operating with three classifiers depending on the message type: connection, subscription, and publication. This approach makes it possible to identify the source of an attack. That can be a network node, a particular device, or a user account. A multi-layer perceptron, the random forest algorithm, and a support vector machine of various configurations were considered as classifiers. Training and test data sets were generated for the proposed feature vector. The classification quality was evaluated by calculating the F1 score, the Matthews correlation coefficient, and accuracy. The multilayer perceptron model and the support vector machine with a polynomial kernel and SMO optimization method showed the best values of all metrics. However, in the case of the support vector machine, a slight decrease in the prediction quality was detected when the width of the traffic analysis window was close to the longest period of sending legitimate messages from the training data set. **Practical relevance:** The results of the research can be used in the development of intrusion detection features for cyberphysical systems using the publish-subscribe model, or other systems based on the same approach.
Keywords — DoS attack, publish-subscribe, machine learning, SVM, random forest, ANN.

For citation: Dikii D. I. DoS attack detection at application level in publish-subscribe networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 4, pp. 50–60 (In Russian). doi:10.31799/1684-8853-2020-4-50–60

References

1. Lee J., Bagheri B., Kao H. A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 2015, vol. 3, pp. 18–23. doi:10.1016/j.mfglet.2014.12.001
2. Henneke D., Elattar M., Jasperneite J. Communication patterns for cyber-physical systems. *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, 2015, pp. 1–4. doi:10.1109/ETFA.2015.7301623
3. Vadlamani S., Eksioglu B., Medal H., Nandi A. Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*, 2016, vol. 172, pp. 76–94. doi:10.1016/j.ijpe.2015.11.008
4. Li Y., Shi L., Cheng P., Chen J., Quevedo D. E. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 2015, vol. 60, no. 10, pp. 2831–2836. doi:10.1109/TAC.2015.2461851
5. Zhang H., Qi Y., Wu J., Fu L., He L. DoS attack energy management against remote state estimation. *IEEE Transactions on Control of Network Systems*, 2018, vol. 5, no. 1, pp. 383–394. doi:10.1109/TCNS.2016.2614099
6. Polyzos G. C., Fotiou N. Building a reliable Internet of things using information-centric networking. *Journal of Reliable Intelligent Environments*, 2015, vol. 1, pp. 47–58. doi:10.1007/s40860-015-0003-5
7. Desnitsky V. A., Kotenko I. V., Rudavin N. N. Protection mechanisms against energy depletion attacks in cyber-physical systems. *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Saint-Petersburg and Moscow, Russia, 2019, pp. 214–219. doi:10.1109/EIConRus.2019.8656795
8. Perrone G., Vecchio M., Pecori R., Giaffreda R. The day after mirai: A survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices. *The 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS)*, 2017, Porto, Portugal, pp. 246–253. doi:10.5220/0006287302460253
9. Dikii D. I. Denial-of-service attack analysis by MQTT protocol. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2020, vol. 20, no. 2, pp. 185–194 (In Russian). doi:10.17586/2226-1494-2020-20-2-185-194
10. Chifor B., Patriciu V. Mitigating DoS attacks in publish-subscribe IoT networks. *The 9th International Conference: Electronics, Computers and Artificial Intelligence (ECAI 2017)*, 2017, pp. 1–6. doi:10.1109/ECAI.2017.8166463
11. Nebbione G., Calzarossa M. Security of IoT application layer protocols: Challenges and findings. *Future Internet*, 2020, vol. 12, no. 55, pp. 1–20. doi:10.3390/fi12030055
12. Haripriya A. P., Kulothungan K. Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *Eurasip Journal on Wireless Communications and Networking*, 2019, vol. 90. doi:10.1186/s13638-019-1402-8
13. Potrino G., De Rango F., Fazio P. A distributed mitigation strategy against DoS attacks in edge computing. *2019 Wireless Telecommunications Symposium (WTS)*, New York City, NY, USA, 2019, pp. 1–7. doi:10.1109/WTS.2019. 8715543
14. Jo H., Jin H. Adaptive periodic communication over MQTT for large-scale cyber-physical systems. *IEEE 3rd International Conference on Cyber-Physical Systems, Networks, and Applications*, 2015, Hong Kong, pp. 66–69. doi:10.1109/CPSNA.2015.21

15. Potrino G., De Rango F., Santamaria A. F. Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker. *IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, Marrakesh, Morocco, 2019, pp. 1–6. doi:10.1109/WCNC.2019.8885553
16. Firdous S. N., Baig Z., Valli C., Ibrahim A. Modelling and evaluation of malicious attacks against the IoT MQTT protocol. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Exeter, 2017, pp. 748–755. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115
17. *OASIS Standart MQTT Version 3.1.1. OASIS*. 2014. 81 p. Available at: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.pdf (accessed 04 April 2020).
18. Gharibian F., Ghorbani A. A. Comparative study of supervised machine learning techniques for intrusion detection. *The Fifth Annual Conference on Communication Networks and Services Research (CNSR '07)*, 2007, Fredericton, NB, pp. 350–358. doi:10.1109/CNSR.2007.22
19. Anbar M., Abdullah R., Hasbullah I. H., Chong Y., Elejla O. E. Comparative performance analysis of classification algorithms for intrusion detection system. *The 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, Auckland, pp. 282–288. doi:10.1109/PST.2016.7906975
20. Barati M., Abdullah A., Udzir N. I., Mahmod R., Mustapha N. Distributed denial of service detection using hybrid machine learning technique. *The International Symposium on Biometrics and Security Technologies (ISBAST)*, 2014, Kuala Lumpur, pp. 268–273. doi:10.1109/ISBAST.2014.7013133
21. Xiao L., Wan X., Lu X., Zhang Y., Wu D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine*, 2018, vol. 35, no. 5, pp. 41–49. doi:10.1109/MSP.2018. 2825478
22. Jianjian D., Yang T., Feiyue Y. A novel intrusion detection system based on IABRBFSVM for wireless sensor networks. *Procedia Computer Science*, 2018, vol. 131, pp. 1113–1121. doi:10.1016/j.procs.2018.04.275
23. Abusitta A., Bellaiche M., Dagenais M. An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. *Journal of Cloud Computing*, 2018, vol. 7, no. 9. doi:10.1186/s13677-018-0109-4
24. Platt J. C. Sequential minimal optimization: A fast algorithm for training support vector machines. *Microsoft Research, Technical Report MSR-TR-98-14*, 1998, pp. 1–21.
25. Hodo E., Bellekens X., Hamilton A., Dubouilh P.-L., Iorkyase E., Tachtatzis C., Atkinson R. Threat analysis of IoT networks using artificial neural network intrusion detection system. *International Symposium on Networks, Computers and Communications (ISNCC)*, Yasmine Hammamet, 2016, pp. 1–6. doi:10.1109/ISNCC.2016.7746067
26. Sangkatsanee P., Wattanapongsakorn N., Charnsripinyo C. Practical real-time intrusion detection using machine learning approaches. *Computer Communications*, 2011, vol. 34, pp. 2227–2235. doi:10.1016/j.comcom.2011.07.001
27. *Paho-MQTT library for Python*. Available at: https://pypi.org/project/paho-mqtt/(accessed 04 April 2020).
28. *Moquette project open source code*. Available at: https://github.com/moquette-io/moquette (accessed 04 April 2020).
29. *WEKA project*. Available at: https://www.cs.waikato.ac.nz/ml/weka/(accessed 04 April 2020).