ИДЕНТИФИКАЦИЯ УГРОЗ ДЛЯ УСТРОЙСТВ МЕДИЦИНСКОГО ИНТЕРНЕТА ВЕЩЕЙ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

DOI: 10.36724/2072-8735-2024-18-12-12-18

Савельева Дарья Дмитриевна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, ***savel.dar.23@mail.ru***

Татарникова Татьяна Михайловна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, ***tm-tatarn@yandex.ru***

Manuscript received 30 October 2024;
Accepted 24 November 2024

Ключевые слова: *методы машинного обучения, анализ трафика, функции защиты информации, интернет вещей, медицинский интернет вещей*

Обсуждается актуальная проблема идентификации угроз в медицинском интернете вещей. В современной медицине устройства медицинского интернета вещей играют важную роль в улучшении качества и доступности медицинских услуг. Они помогают в диагностике, мониторинге состояния пациентов и проведении медицинских процедур. С другой стороны, рост использования медицинского интернета вещей приводит к увеличению рисков кибератак, которые могут иметь серьезные последствия для здоровья пациентов и работы медицинских учреждений. Сетевые атаки на медицинский интернет вещей могут привести к утечке конфиденциальной информации, нарушению работы жизненно важных систем мониторинга и даже к угрозе жизни пациентов. Поэтому обеспечение безопасности медицинского интернета вещей является важной задачей для исследователей, разработчиков и медицинских организаций. Одним из перспективных подходов к обеспечению безопасности медицинского интернета вещей является использование методов машинного обучения для обнаружения и идентификации сетевых атак в трафике, передаваемом между пациентами и медицинским учреждением. Машинное обучение позволяет создавать модели, способные автоматически обучаться на основе анализа большого объема данных и выявлять аномалии в трафике, которые могут указывать на наличие сетевой атаки. В статье приведена инфраструктура медицинского интернета вещей и рассмотрены протоколы передачи трафика, позволяющие увидеть уязвимые к атакам участки передачи данных. Выполнена программная реализация нескольких популярных алгоритмов машинного обучения, которые могут быть использованы для детектирования сетевых атак в трафике медицинского интернета вещей. Наиболее эффективный с точки зрения метрик классификации алгоритм машинного обучения рекомендуется для реализации в виде системы обнаружения вторжений на каждом узле приема трафика – координаторе, базовых станциях, маршрутизаторах и брандмауэрах.

Информация об авторах:
Савельева Дарья Дмитриевна, *Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра информационных систем и технологий, аспирант, г. Санкт-Петербург, Россия*
Татарникова Татьяна Михайловна, *Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра прикладной информатики, д.т.н., профессор, г. Санкт-Петербург, Россия*

Для цитирования:
Савельева Д.Д., Татарникова Т.М. Идентификация угроз для устройств медицинского интернета вещей методами машинного обучения // T-Comm: Телекоммуникации и транспорт. 2024. Том 18. №12. С. 12-18.

For citation:
Savelyeva D.D., Tatarnikova T.M. (2024) Identification of threats to medical internet of things devices using machine learning methods. *T-Comm*, vol. 18, no.12, pp. 12-18. (*in Russian*)

Введение

В современном мире интернет вещей (IoT) стал неотъемлемой частью нашей жизни, проникая во все сферы деятельности, включая медицину. Развитие технологий и увеличение количества подключенных устройств привели к возникновению новой области – медицинского интернета вещей (IoMT), который представляет собой интеграцию IoT-технологий в медицинскую практику [1].

Сенсорные устройства могут быть интегрированы в наручные часы, браслеты, мобильные терминалы, прикреплены к одежде, размещены на теле человека, а также имплантированы под кожу, что обеспечивает беспроводный мониторинг в любом месте и в любое время [2]. Пациенту совсем необязательно физически быть на приеме у врача, если происходит рутинная диагностическая проверка – нетельные беспроводные сенсорные устройства передают измерения, аккумулируемые координатором (например смартфоном) в информационный центр медицинского учреждения. В свою очередь, лечащий врач через процедуру авторизации получает доступ к данным пациента и использует ресурсы центра для предиктивной аналитики (рис. 1).

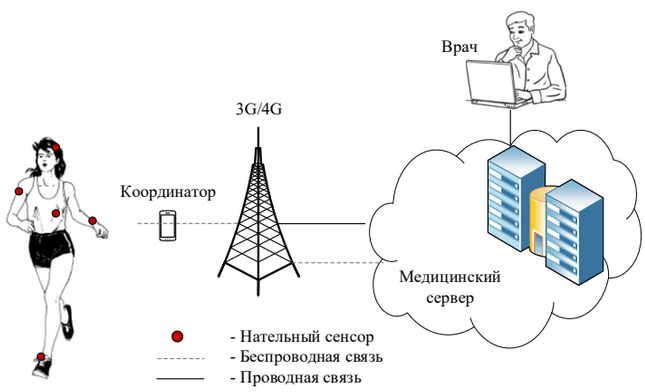

Рис. 1. Инфраструктура медицинского интернета вещей

IoMT открывает широкие возможности для улучшения качества и доступности медицинских услуг. С его помощью можно осуществлять диагностику, мониторинг пациентов и проведение медицинских процедур, что особенно актуально для отдаленных и недостаточно обеспеченных медицинскими учреждениями регионов. Типичными примерами применения интернета вещей в медицине являются следующие [3]:

– Учет медицинского оборудования и ресурсов;
– Дистанционная медицинская помощь
– Индикаторы падения пациентов;
– Спортивная медицина;
– Предиктивная аналитика с носимых устройств;
– Наблюдение и уход за пожилыми пациентами.

Однако вместе с преимуществами IoMT возникают и новые риски, связанные с безопасностью и защитой данных.

Кибератаки на системы IoMT могут привести к серьезным последствиям, включая угрозу жизни пациентов. Утечки конфиденциальной медицинской информации могут нарушить право пациентов на защиту персональных данных и подорвать доверие к системе здравоохранения.

Кроме того, жизненно важные системы мониторинга могут стать объектом атак, направленных на нарушение их функционирования [4].

Протоколы передачи данных в медицинском интернете вещей

В медицинском секторе интернета вещей применяются три стандарта передачи данных [5]:

– стандарты серии IEEE 802.11, известные как Wi-Fi. Оборудование Wi-Fi является наиболее массовым и в радиусе его действия позволяет обеспечить доступ к сети Интернет;

– протокол MQTT (Message Queue Telemetry Transport), устанавливающий правила сбора данных от множества сенсорных устройств и передачу их на сервер. В качестве транспорта – протокол TCP. Протокол MQTT основывается на модели издатель-подписчик с использованием промежуточного сервера – брокера. Брокер решает задачу формирования очередей сообщений и их приоритезацию. Таким образом, вся передаваемая информация разделяется по направлениям на разные каналы, число которых соответствует количеству издателей/подписчиков. Все сенсорные или исполнительные устройства посылают данные только брокеру и принимают данные тоже только от него. То есть, когда один клиент, так называемый издатель, передает сообщение *M* на определенную тему *T*, то все клиенты, которые подписываются на тему *T*, получают это сообщение *M*. Например, три клиента подключены к брокеру, клиенты *B* и *C* подписываются на topic «Temperature» (рис. 2). В какое-то время, когда клиент *A* передает значение «30» на topic «Temperature» (рис. 2, *а*), сразу после его получения брокер передает это сообщение к подписавшимся клиентам (рис. 2, *б*). Также в MQTT предусматривается выбор надежности обмена сообщениями, которые обеспечиваются уровнями качества обслуживания (QoS, Quality of Service);

– стандарты серии IEEE 802.15, известные как Bluetooth. Оборудование Bluetooth реализует обмен данными между различными устройствами на небольшие расстояния до нескольких десятков метров. Небольшой радиус действия устройств с Bluetooth-интерфейсом позволяет развернуть работу локального участка медицинского интернета вещей на ограниченной площади, например в рамках квартиры, офисного рабочего места, нательной медицинской сети.

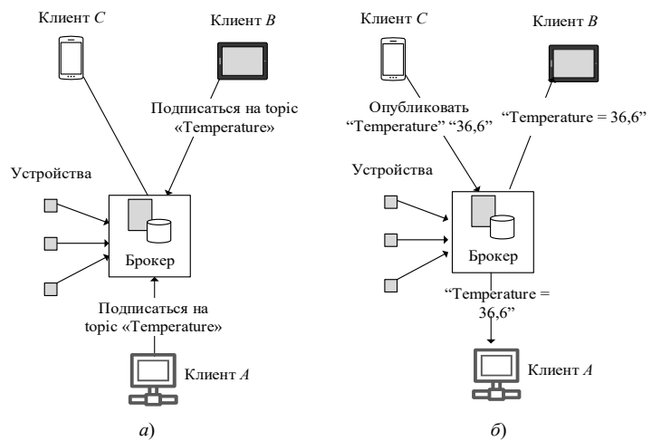

Рис. 2. Схема работы протокола MQTT

Таким образом, в инфраструктуре медицинского интернета вещей существуют открытые участки передачи данных, требующие своевременного обнаружения аномального трафика в виде сетевых атак.

Идентификация угроз методом машинного обучения

Системы обнаружения и идентификации сетевых атак в трафике устройств Интернета вещей разделяются на три вида, основанных на [6]:

1) статистическом методе обнаружения аномалий в трафике устройств интернета вещей, при котором осуществляется анализ характеристик сетевого трафика с целью выявления отклонений от ожидаемого поведения. Этот метод обнаруживает необычные паттерны или события, которые могут указывать на наличие атаки;

2) машинном обучении, предполагающем использование алгоритмов для выявления аномалий с применением обучения на размеченных данных. Система анализирует большой объем нормального (не аномального) трафика и создает модель, которая в последствии используется для обнаружения аномального трафика в реальном времени.

3) Гибридном решении, которое объединяет статистический метод и машинное обучение для повышения эффективности обнаружения атак. Оно может использовать преимущества обоих методов и компенсировать их недостатки.

Каждый из этих методов имеет свои преимущества и недостатки, и выбор конкретного из них зависит от требований и условий реализуемой системы обнаружения и идентификации сетевых атак [7,8]. В данной статье рассматривается метод обнаружения сетевой атаки с применением машинного обучения.

Преимущества идентификации атаки методом машинного обучения:

– высокая точность: алгоритмы машинного обучения способны выявлять даже незначительные отклонения от нормального поведения трафика, что позволяет обнаруживать различные типы атак;

– способность к обучению: система может обучаться на размеченных данных, что позволяет ей адаптироваться к изменениям в трафике и улучшать свои способности к обнаружению аномалий;

– автоматизация: после обучения система может автоматически обнаруживать аномалии в реальном времени, что позволяет оперативно реагировать на угрозы;

– гибкость: можно использовать различные алгоритмы машинного обучения в зависимости от требований и условий конкретной системы обнаружения атак.

Этапы метода машинного обучения для нахождения аномалий в трафике [9]:

1) подготовка данных: необходимо собрать данные о нормальном трафике для обучения модели. Это могут быть данные о трафике за определённый период времени или данные, полученные в результате симуляции нормального трафика. В данной статье обучение происходит на готовом наборе данных.

2) предобработка исходного набора данных: нормализация и разделения данных для обучения и тестирования.

3) выбор алгоритма машинного обучения: определение наиболее эффективного для реализации алгоритма согласно требованиям к точности, скорости работы и других факторов.

4) обучение модели: на основе собранных данных модель обучается выявлять нормальные паттерны трафика.

5) тестирование модели: после обучения модель тестируется на данных, которые не использовались для обучения. Это позволяет оценить её точность и способность к обнаружению аномалий.

В настоящем исследовании использован исходный набор данных CIC IoMT 2024 от Канадского Института Кибербезопасности, представляющий собой эталонные данные для разработки и оценки решений по обеспечению безопасности в интернете медицинских вещей (IoMT). Для этого было проведено 18 атак на тестовую среду IoMT, состоящую из 40 устройств IoMT (25 реальных устройств и 15 смоделированных устройств), с учетом множества протоколов, используемых в здравоохранении, таких как Wi-Fi, MQTT и Bluetooth.

Характеристика применяемых методов машинного обучения

Для построения модели детектирования угроз были рассмотрены следующие варианты:

Дерево решений (Decision Tree, DR). Деревья решений состоят из узлов и ветвей, которые представляют правила принятия решений. Каждый узел соответствует условию, а каждая ветвь – результату этого условия. Чем глубже дерево, тем больше условий и, соответственно, точнее модель.

Пусть X есть множество объектов, их количество – есть мощность множества $|X|=n$. Обозначим множество классов (метки класса) $C=\{C_1, C_2, \ldots, C_k\}$ и множество признаков $A=\{A_1, A_2, \ldots, A_m\}$. Тогда решающее дерево разбивает все признаковое пространство A на некоторое количество непересекающихся подмножеств $\{X_1, \ldots, X_k\}$ и каждое подмножество ставится в соответствие классу C_i.

Процесс конструирования дерева решений состоят из двух этапов: индукции – построения дерева: решаются вопросы выбора критерия расщепления дерева на ветви и остановки обучения, если это предусмотрено алгоритмом; отсечения – регулирования глубины дерева: решается вопрос отсечения некоторых его малоинформативных ветвей.

Качество построенного дерева решения зависит от выбранного критерия расщепления. Наиболее известный – мера энтропии, которая используется в данной работе для выбора признака, обладающего наибольшей информативностью из имеющегося пространства признаков

$$H(x) = -\sum_{i=1}^{N} p(i)\log_2 p(i), \qquad (1)$$

Деревья решений обладают рядом преимуществ, среди основных – это простота восприятия и интерпретации. Основной недостаток – это проблема обучения оптимального дерева решений, которая является NP-полной задачей даже для простых концепций.

Случайный лес (Random Forest, RF). Это метод машинного обучения, который объединяет несколько решающих деревьев для получения более точных и устойчивых результатов. Случайный лес создает ансамбль из множества решающих деревьев, где каждое дерево обучается на случайной выборке данных и случайном подмножестве признаков, что позволяет

уменьшить переобучение и повысить обобщающую способность модели. Каждое дерево в случайном лесу обучается на уникальных данных и признаках, что приводит к разнообразию моделей в ансамбле. Итоговый результат случайного леса формируется путем усреднения предсказаний всех деревьев в ансамбле.

Обобщенный алгоритм случайного леса включает следующие шаги:

1. Выбрать число деревьев – классификаторов, пусть это N деревьев.

2. Для каждой модели дерева решений G_i, $i=\overline{1,N}$ выбрать число признаков k ($k \le K$, где K – общее количество признаков) для обучения. Обычно для всех моделей используется только одно значение k.

3. Для каждого дерева G_i, $i=\overline{1,N}$ создать обучающую выборку и обучить модель.

4. Объединить результаты отдельных G_i, $i=\overline{1,N}$ деревьев мажоритарным голосованием, то есть за итоговый классификатор принять

$$\mathbf{G}(\mathbf{X}) = \arg\max \sum_{i=1}^{N} \mathbf{G}_i(\mathbf{X}).$$

Основное достоинства данной модели случайного леса – это высокая устойчивость к переобучению и выбросам благодаря разнообразию деревьев в ансамбле и усреднению предсказаний. Основной недостаток – это сложная интерпретация из-за большого количества деревьев и их разнообразия,

Ансамблевые методы. Это методы машинного обучения, объединяющие несколько базовых моделей. В данной работе рассматривались только ансамбли деревьев решений, обучаемые по технологии boosting.

Boosting – это техника обучения деревьев решений для сборки их в сильный классификатор, при котором неверно классифицированные примеры обучения получают больший вес, а правильно классифицированные примеры теряют вес, что позволяет при дальнейшем обучении сфокусироваться на ошибочно классифицированных примерах.

Обобщенный алгоритм обучения по технологии boosting предполагает следующие шаги:

1. Выбрать число деревьев – слабых классификаторов, пусть это N деревьев.

2. Для каждого i=1, …, N сгенерировать выборку X_i с помощью bagging и построить решающее дерево G_i по выборке X_i.

3. Оценить ошибку, если она соответствует допустимой, то переход к п. 5.

4. Найти информативный признак для расщепления, переход к п. 3.

5. Завершить построение классификатора.

В работе представлены три модели обучения по технологии boosting:

– Модель градиентного бустинга XGBClassifier;

– Модель градиентного CatBoostClassifier;

– Модель стохастического градиентного спуска SGDClassifier.

Основное достоинство данных моделей – это эффективность работы с большими данными на многоядерных процессорах и графических процессорах. Основной недостаток модели – сложная настройка параметров алгоритма, требующей экспериментов и тестирования.

Сверточная сеть (Convolutional neural network, CNN). Это тип архитектуры искусственных нейронных сетей, который успешно применяется для анализа и обработки изображений. В данной работе такими изображениями являются графики зависимости основных характеристик трафика, на которых строится эталонный паттерн. CNN используются сверточные слои, которые выполняют операцию свертки над входными данными с набором фильтров. Назначение сверточных слоев – выделить признаки на входном изображении и сформировать карту признаков, при этом один фильтр определяет конкретную характеристику.

Сверточная нейронная сеть обучается с помощью алгоритма обратного распространения ошибки. Сначала выполняется прямое распространение от первого слоя к последнему, после чего вычисляется ошибка на выходном слое и распространяется обратно. При этом на каждом слое вычисляются градиенты обучаемых параметров, которые в конце обратного распространения используются для обновления весов с помощью градиентного спуска. Основные достоинства CNN заключаются в том, что она может обучаться на больших объемах данных, что позволяет ей лучше выделять важные признаки и структуры, а также показывает высокую точность на задачах классификации.

Недостатки CNN типичны для искусственных нейронных сетей: результаты работы сложно интерпретировать, поскольку она работает с высокоуровневыми признаками и структурами и для обучения CNN требуется большой объем размеченных данных, что может быть проблематично для некоторых задач.

Логистическая регрессия (Logistic Regression, LR). Это метод машинного обучения, который основан на логистической функции, преобразующей линейную комбинацию независимых переменных в вероятность.

Основное достоинство линейной регрессии – это возможность стабилизации с помощью регуляризации, что помогает предотвратить переобучение и улучшить обобщающую способность модели. Основной недостаток – это недостаточная гибкость для моделирования сложных зависимостей между переменными.

Метрики эффективности методов машинного обучения

Для оценивая эффективности работы моделей были использованы следующие метрики [10]:

– точность классификации, показывает долю, в %, верной классификации

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \quad (2)$$

где TP (True positive – истинно-положительное решение) – число раз, когда результат предсказания моделью положительного класса объекта совпал с реальной меткой класса;

FP (False Positive – ложноположительное решение или ошибка 1-го рода) – число раз, когда модель ошибочно отнесла объект к положительному классу, который на самом деле относится к отрицательному классу;

FN (False Negative – ложноотрицательное решение или ошибка 2-го рода) – число раз, когда модель ошибочно классифицировала отрицательный объект, как положительный.

TN (True Negative – истинно-отрицательное решение) – число раз, когда модель классифицировала объект как отрицательный, каким он является в действительности

– сбалансированная точность (Balanced Accuracy, BA), применяемая в случае дисбаланса классов

$$\mathrm{BA} = \frac{1}{2}\left(\frac{TP}{TP+FN} + \frac{TN}{TN+FP}\right). \quad (3)$$

F-мера (Fscore) сочетает в себе оценки точности и полноты

$$\mathrm{Fscore} = \frac{2 \cdot \mathrm{recall} \cdot \mathrm{precision}}{\mathrm{recall}+\mathrm{precision}}, \quad (4)$$

где recall – доля истинно положительных решений, называемая также полнотой – пропорция отрицательных объектов, классифицированных корректно во всем множестве отрицательных объектов, представленных в выборке

$$\mathrm{Recall} = \frac{TP}{TP+FN}. \quad (5)$$

В (4) точности и полноте отдается одинаковый вес, поэтому F-мера будет снижаться одинаково при уменьшении и точности и полноты.

– время работы модели (time) – время обучения алгоритма, [c].

Первые три метрики были собраны с помощью библиотеки metrics из библиотеки sklearn, а метрика времени – с помощью пакета time.

Scikit-learn (или sklearn) – это широко известная библиотека для языка Python, которая предлагает реализацию разнообразных алгоритмов машинного обучения и инструменты для их использования. Библиотека позволяет использовать различные алгоритмы машинного обучения, метрики для оценивания для эффективности, а также инструменты для предварительной обработки данных (представлены далее).

Данные в выбранном датасете изначально разделены для обучения и тестирования. При использовании первоначального разделения и нормализации данных с помощью библиотеки MinMaxScaler из sklearn получены результаты, представленные в таблице 1.

Таблица 1

Результаты с нормализацией MinMaxScaler

Метод	Accuracy	BA	Fscore	Time
DR	0,977685	0,929869	0,977685	49,110897
RF	0,973764	0,977045	0,973764	383,27684
XGBClassifier	0,977118	0,922868	0,977118	458,821513
CatBoostClassifier	0,974629	0,986891	0,974629	7,839376
SGDClassifier	0,973065	0,967742	0,973065	11,726824
CNN	0,973093	0,986363	0,973093	2294.000035
LR	0,973400	0,965380	0,973400	6,991560

При использовании первоначального разделения и нормализации данных с помощью библиотеки StandardScaler из sklearn получены результаты, представленные в таблице 2.

Таблица 2

Результаты с нормализацией StandardScaler

Метод	Accuracy	BA	Fscore	Time
DR	0,954595	0,944287	0,954595	32,269734
RF	0,966321	0,982636	0,966321	297,632969
XGBClassifier	0,960463	0,978477	0,960463	411,534630
CatBoostClassifier	0,961942	0,966308	0,961942	6,243363
SGDClassifier	0,896366	0,947211	0,896366	10,237078
CNN	0,988485	0,500000	0,988485	2678.680091
LR	0,946100	0,971970	0,946100	21,473670

При слиянии первоначально выделенных данных для тестирования и обучения и разделения уже с помощью функции train_test_split(test_size=.25) пакета model_selection и нормализации данных с помощью пакета normalize из библиотеки sklearn получены результаты, представленные в таблице 3.

Таблица 3

Результаты с нормализацией Normalize

Метод	Accuracy	BA	Fscore	Time
DR	0,978204	0,861586	0,978204	109,372993
RF	0,971387	0,745396	0,971387	433,509614
XGBClassifier	0,989699	0,941434	0,989699	912,138282
CatBoostClassifier	0,987691	0,928863	0,987691	244,869112
SGDClassifier	0,971351	0,744884	0,971351	26,926438
CNN	0,971370	0,744928	0,971370	3928.639033
LR	0,971270	0,741059	0,971270	15,898890

Из полученных результатов применения методов машинного обучения при различных методах нормализации данных напрашиваются следующие выводы:

1) Самой быстрой во всех случаях обучения стала модель логистической регрессии.

2) В случае с нормализацией MinMaxScaler по точности Accuracy и оценке Fscore выигрывает модель дерева решений, а по сбалансированной точности BA – модель CatBoostClassifier.

3) В случае с нормализацией StandardScaler по обычной точности Accuracy и оценке Fscore выигрывает модель сверточной сети CNN, а по сбалансированной точности BA – модель случайного леса.

4) В случае с изменёнными данными для тестирования и обучения с нормализацией normalize выигрывает по всем метрикам модель градиентного бустинга XGBClassifier.

Заключение

Рассмотрены методы машинного обучения для бинарной классификации трафика медицинского интернета вещей. Каждый метод был рассмотрен с учетом их достоинств и недостатков, а также по метрикам эффективности каждой модели: точность, сбалансированная точность, F-мера и время работы.

В качестве исходного набора данных использовался открытый датасет CIC IoMT 2024, который содержит наиболее актуальные данные.

При разных способах предобработки данных с первоначальной разбивкой получены разные по точности результаты: наиболее эффективными классификаторами являются

модели дерева решений, случайного леса, градиентного бустинга CatBoostClassifier и сверточной сети CNN.

При новой разбивке по всем параметрам точности выигрывает модель градиентного бустинга XGBClassifier.

Самой быстро обучаемой моделью стала модель логистической регрессии.

На всех экспериментах минимальную точность accuracy продемонстрировала модель стохастического градиентного спуска SGDClassifier (0,896), а максимальную – модель XGBClassifier (0,989).

Таким образом, для идентификации угроз для устройств медицинского интернета вещей методами машинного обучения по комплексу всех оцениваемых метрик может быть рекомендована логистическая регрессия. Программная реализация алгоритма логистической регрессии может быть реализована в виде системы обнаружения вторжений на каждом узле приема трафика – координаторе, базовых станциях, маршрутизаторах и брандмауэрах.

Литература

1. *Кучерявый А.Е., Бородин А.С., Киричек Р.В.* Сети связи 2030 // Электросвязь. 2018. Т. 11. С. 52-56.

2. *Аксенова Е.И., Горбатов С.Ю.* Применение технологий интернета вещей в здравоохранении // Здоровье мегаполиса. 2021. №4. С. 101-113. doi: 10.47619/2713-2617.zm.2021.v2i4

3. *Поторочина К.Л., Никитина Е.Ю.* Безопасность применения IoT в сфере здравоохранения // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2022. №4 (59). С. 68-81. DOI: .17072/1993-0550-2022-4-68-81/

4. *Муренин И.Н.* Обнаружение аномалий в трафике устройств Интернета вещей // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 128-137. DOI:10.31854/1813-324X-2021-7-4-128-137.

5. *Lee Perry*. Internet of Things Architects. Packt Publishing, 2018. 514 p.

6. *Сахаров Д.В., Козлов Д.С.* Обнаружение аномального поведения устройства IoT в сети на основе модели трафика // Информационные технологии и телекоммуникации. 2019. Т. 7, № 3. С. 50-55. DOI 10.31854/2307-1303-2019-7-3-50-55.

7. *Татарникова Т.М., Бимбетов Ф., Богданов П.Ю.* Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. №4. С. 36-41.

8. *Нианг П.М., Сидоренко В.Г.* Выбор алгоритма машинного обучения для обнаружения вторжений в IoT // Надежность. 2024. Т. 24(3). С. 44-51. DOI: 10.21683/1729-2646-2024-24-3-44-51

9. *Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, Jake Vanderplas, Alexandre Passos, David Cournapeau, Matthieu Brucher, Matthieu Perrot, Edouard Duchesnay*. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. 2011. 12(85), pp. 2825-2830.

10. *Татарникова Т.М., Богданов П.Ю.* Метрические характеристики обнаружения аномального трафика в сетях интернета вещей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 15. №1. С. 15-21.

IDENTIFICATION OF THREATS TO MEDICAL INTERNET OF THINGS DEVICES USING MACHINE LEARNING METHODS

Daria D. Savelyeva, *Saint-Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia,* ***savel.dar.23@mail.ru***

Tatyana M. Tatarnikova, *Saint-Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia,* ***tm-tatarn@yandex.ru***

Abstract

The article discusses the current problem of identifying threats in the medical Internet of Things. In modern medicine, medical Internet of Things devices play an important role in improving the quality and availability of medical services. They help in diagnostics, monitoring the condition of patients and performing medical procedures. On the other hand, the growing use of the medical Internet of Things leads to an increase in the risk of cyberattacks, which can have serious consequences for the health of patients and the operation of medical institutions. Network attacks on the medical Internet of Things can lead to the leakage of confidential information, disruption of vital monitoring systems and even a threat to the lives of patients. Therefore, ensuring the security of the medical Internet of Things is an important task for researchers, developers and medical organizations. One of the promising approaches to ensuring the security of the medical Internet of Things is the use of machine learning methods to detect and identify network attacks in traffic transmitted between patients and a medical institution. Machine learning allows you to create models that can automatically learn based on the analysis of large amounts of data and identify anomalies in traffic that may indicate a network attack. The article provides the infrastructure of the medical Internet of Things and discusses traffic transmission protocols that allow you to see areas of data transmission vulnerable to attacks. Software implementation of several popular machine learning algorithms has been completed, which can be used to detect network attacks in medical Internet of Things traffic. The most effective machine learning algorithm in terms of classification metrics is recommended for implementation as an intrusion detection system at each traffic receiving node - the coordinator, base stations, routers and firewalls.

Keywords: *machine learning methods, traffic analysis, information security functions, Internet of things, medical Internet of things.*

References

[1] A. Eu. Koucheryavy, A. S. Borodin, R. V. Kirichek, "Network 2030," *Telecommunications and Radio Engineering*, 2018, vol. 11, pp. 52-56. (In Russian)
[2] E. I. Aksenova, S. Yu. Gorbatov, "Application of IoT technologies in healthcare," *City Healthcare*, 2021, vol. 2(4), pp. 101-113. DOI: 10.47619/2713-2617.zm.2021.v2i4;101-113. (In Russian)
[3] K. L. Potorochina, E. Yu. Nikitina, "Security of IoT Applications in Health Care," *Bulletin of Perm University. Mathematics. Mechanics. Computer Science*, 2022, vol. 4(59), pp. 68-81. DOI: 10.17072/1993- 0550-2022-4-68-81. (In Russian)
[4] I. Murenin, "Detection of Anomalies in the Traffic of IoT Devices," *Proc. of Telecom. Universities*, 2021, vol. 7(4), pp. 128-137. DOI:10.31854/ 1813-324X-2021-7-4-128-137. (in Russian)
[5] *Lee Perry*, "Internet of Things Architects," Packt Publishing, 2018, 514 p.
[6] D. Saharov, D. Kozlov, "Detecting Abnormal Behavior of an IoT Device in the Network Based on a Traffic Model," *Telecom IT*, 2019, vol. 7, Iss. 3, pp. 50-55. DOI 10.31854/2307-1303-2019-7-3-50-55. (in Russian)
[7] T. M. Tatarnikova, F. Bimbetov, P. Yu. Bogdanov, "Detection of network traffic anomalies by deep learning," *Izvestiya SPbGETU LETI*, 2021, no. 4, pp. 36-41 (In Russian).
[8] P. M. Niang, V. G. Sidorenko, "Choosing the machine learning algorithm for detecting intrusions into IoT," *Dependability*, 2021, vol. 24(3), pp. 44-51. https://doi.org/10.21683/1729-2646-2024-24-3-44-51. (In Russian)
[9] Fabian Pedregosa, Gael Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, Jake Vanderplas, Alexandre Passos, David Cournapeau, Matthieu Brucher, Matthieu Perrot, Edouard Duchesnay, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, 2011, vol. 12(85), pp. 2825-2830.
[10] T. M. Tatarnikova, P. Yu. Bogdanov, "Metric characteristics of anomalous traffic detection in internet of things," *T-Comm*, 2022, vol. 15, no.1, pp. 15-21. (in Russian)

Information about authors:

Daria D. Savelyeva, *graduate student, Petersburg State University of Aerospace Instrumentation, Institute of Information Technology and Programming, St. Petersburg, Russia*

Tatyana M. Tatarnikova, *Doctor of Technical Sciences, Professor, St. Petersburg State University of Aerospace Instrumentation, Institute of Information Technology and Programming, St. Petersburg, Russia*