УДК 004.72
doi: 10.21685/2227-8486-2023-3-9

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ СЕНСОРНЫХ ДАННЫХ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ И НЕЙРОННОЙ СЕТИ В СИСТЕМЕ МОНИТОРИНГА КРИТИЧЕСКИХ СОБЫТИЙ

А. А. Финогеев

Пензенский государственный университет, Пенза, Россия
fanton3@yandex.ru

Аннотация. *Актуальность и цели.* Рассматриваются вопросы интеллектуального анализа сенсорных данных в защищенной архитектуре системы мониторинга критических событий в дорожной инфраструктуре. *Материалы и методы.* Для интеллектуального анализа, кластеризации и распознавания пакетов предлагается комбинированный подход, который реализуется в архитектуре программно-конфигурируемой сети. Подход включает процедуры фильтрации недопустимого трафика, валидации подлинности сетевых узлов, метод интеллектуального анализа распознавания и кластеризации пакетов сенсорных данных на основе аппарата нечеткой логики и пятислойной нейронной сети в пространстве девяти признаков. Функции принадлежности к нетипичным пакетам настраиваются в процессе обучения нейронной сети, а вывод о степени сходства формируется с помощью аппарата нечеткой логики. *Результаты.* Предложена архитектура защищенной системы мониторинга с четырьмя слоями и шестью уровнями управления данными. В архитектуре предусмотрена подсистема интеллектуального анализа и кластеризации, которая включает модули валидации сетевых узлов и фильтрации трафика, парсер и анализатор пакетов на базе нечеткой логики и нейронной сети, модуль журнализации. *Выводы.* Преимуществами предложенной системы мониторинга являются: архитектура программно-конфигурируемой сети, встроенные механизмы анализа сетевого трафика, метод распознаваний и кластеризации пакетов, способ валидации сетевых узлов, методика фильтрации недопустимого трафика от скомпрометированных узлов.

Ключевые слова: система мониторинга, программно-конфигурируемая сеть, сенсорные данные, нечеткая логика, нейронная сеть, кластеризация

Финансирование: исследование выполнено при поддержке гранта Российского научного фонда (проект № 20-71-10087).

Для цитирования: Финогеев А. А. Интеллектуальный анализ сенсорных данных на основе нечеткой логики и нейронной сети в системе мониторинга критических событий // Модели, системы, сети в экономике, технике, природе и обществе. 2023. № 3. С. 125–141. doi: 10.21685/2227-8486-2023-3-9

INTELLIGENT ANALYSIS OF SENSORY DATA BASED ON FUZZY LOGIC AND NEURAL NETWORK IN CRITICAL EVENT MONITORING SYSTEMS

A.A. Finogeev

Penza State University, Penza, Russia
fanton3@yandex.ru

Abstract. *Background*. The article deals with the issues of intellectual analysis of sensory data in a secure architecture of a system for monitoring critical events in the road infrastructure. *Materials and methods*. For intellectual analysis, clustering and packet recognition, a combined approach is proposed, which is implemented in the architecture of a software-defined network. The approach includes procedures for filtering invalid traffic, validating the authenticity of network nodes, a method of intellectual analysis of recognition and clustering of sensor data packets based on a fuzzy logic apparatus and a five-layer neural network in the space of nine features. The function of belonging to atypical packages is adjusted in the process of training the neural network, and the conclusion about the degree of similarity is formed using the fuzzy logic apparatus. *Results*. The architecture provides for a subsystem of intellectual analysis and clustering, which includes modules for validating network nodes and traffic filtering, a parser and packet analyzer based on fuzzy logic and a neural network, and a logging module. *Conclusions*. The advantages of the proposed monitoring system are: software-defined network architecture, built-in network traffic analysis mechanisms, packet recognition and clustering method, network node validation method, invalid traffic filtering method from compromised nodes.

Keywords: monitoring system, software defined network, sensor data, fuzzy logic, neural network, clustering

Acknowledgements: the study was supported by a grant from the Russian Scientific Foundation (project № 20-71-10087).

For citation: Finogeev A.A. Intelligent analysis of sensory data based on fuzzy logic and neural network in critical event monitoring systems. *Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve = Models, systems, networks in economics, technology, nature and society*. 2023;(3):125–141. (In Russ.). doi: 10.21685/2227-8486-2023-3-9

Введение

Внедрение технологий Интернета вещей (IoT) в различные сферы человеческой жизнедеятельности привело к широкому распространению межмашинного взаимодействия. Увеличение числа таких взаимодействий между узлами сенсорных сетей привело к росту угроз информационной безопасности [1]. Повышение риска информационных атак связано с ростом количества киберфизических устройств IoT и мобильных средств связи для доступа к данным по распределенным телекоммуникационным каналам [2]. Наибольшую угрозу в открытых сетевых системах представляют атаки флудинга в виде генерации большого числа запросов к сетевым узлам [3]. Для защиты распределенных систем мониторинга предлагается использовать интеллектуальную подсистему анализа сетевого трафика на основе аппарата нечеткой логики и нейронной сети.

Сбор, обработка и хранение данных являются основными операциями в системах мониторинга критических событий на пространственно-распределенных объектах дорожно-транспортной инфраструктуры [4]. Подобные системы работают с большими сенсорными данными, которые содержат информацию о дорожно-транспортных происшествиях и нарушениях правил дорожного движения [5]. Данные собираются с множества фоторадарных комплексов фото- и видеофиксации инцидентов, а также с камер видеонаблюдения, которые объединены единой сетевой инфраструктурой в рамках концепций «Безопасный город» и «Безопасные дороги».

В последнее время исследователи предлагают способы использования архитектуры программно-конфигурируемых сетей (Software Defined Network –

SDN) для защиты сетевых систем [6, 7]. Внедрение архитектуры SDN-сети для создания транспортной среды обусловлено необходимостью применения новых подходов к обнаружению и предотвращению угроз информационной безопасности. SDN-технология представляет собой централизованный способ управления и настройки сетевых коммутаторов, который позволяет минимизировать риски и последствия информационных атак [8, 9]. Основная идея сводится к отделению уровня логического управления сетью от уровня коммутации и ретрансляции пакетов данных в коммутаторах [10]. Однако SDN-архитектура имеет ряд ограничений. Во-первых, следует отметить проблему масштабируемости SDN из-за централизации управления потоками данных в контроллере [11]. Во-вторых, в случае распределенных DDoS-атак контроллер не успевает обрабатывать входящие запросы и генерировать новые правила таблиц потоков для коммутаторов [12]. В связи с этим для эффективного использования SDN-архитектуры необходимы методы и средства обнаружения атак на основе технологий машинного обучения, интеллектуального и статистического анализа, нейронных сетей [2, 13].

В работе [14] авторами сделан обзор решений для обнаружения и предотвращения DDoS-атак с использованием SDN-архитектуры и предложена платформа проактивного обнаружения подобных атак в корпоративных сетях. В статье [15] для защиты IoT сетей предлагается использование SDN, блокчейн и технологии виртуализации сетевых функций. Авторами представлен обзор решений по безопасности с констатацией таких проблем, как отсутствие стандартизации, низкая эффективность выявления вредоносного трафика, большие задержки при росте числа атак. Архитектура SDN в работе [16] позволяет обнаруживать DDoS-атаки в режиме реального времени с минимальными требованиями к производительности сетевых узлов, что важно для сенсорных сетей низкого энергопотребления. В статье [17] рассмотрена процедура обнаружения флудинг-атак в кэше данных SDN-контроллера. Атаки выявляются в процессе обмена данными между генерирующими устройствами и счетчиками электроэнергии у потребителей. В работе [18] предлагается SDN-архитектура гетерогенной сети, состоящей из мобильных устройств связи, коммутаторов и контроллеров с системой распределенного реестра (блокчейн), которая применяется для шифрования пакетов сенсорных данных перед передачей на сервер и доказательства их подлинности.

Разработанная на основании изученного опыта, в статье представлена архитектура защищенной системы мониторинга критических событий, создаваемой с использованием технологии программно-конфигурируемой сети (SDN), интеллектуального анализа, распознавания и кластеризации пакетов сетевого трафика на основе нечеткой логики и многослойной нейронной сети, технологии распределенного реестра для хранения данных, смарт-контрактов для валидации сетевых узлов, синтеза правил таблиц потоков, анализа и фильтрации сетевого трафика.

Материалы и методы

Основная функция подсистемы защиты операций по сбору и передаче сетевого трафика от распределенных узлов в системе мониторинга состоит в анализе пакетов данных от авторизованных узлов с целью обнаружения нетипичных пакетов с возможным вредоносным содержимым. Архитектура разработанной подсистемы анализа трафика включает парсер, анализатор, модуль кластеризации с нейронной сетью, модуль журнализации (рис. 1).

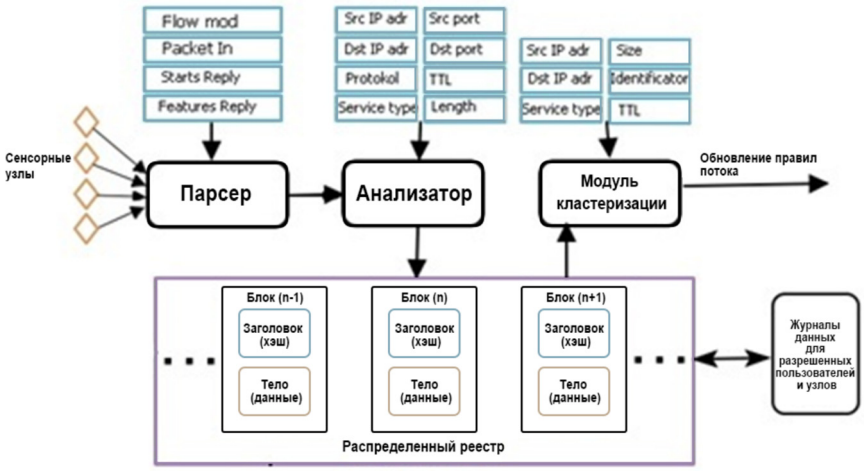

Рис. 1. Подсистема анализа и обнаружения нетипичных пакетов данных

Модули парсинга и интеллектуального анализа необходимы для обнаружения пакетов данных, характеристики которых отличаются от тех, которые обычно передаются от авторизованных узлом. Процедура анализа реализуется в контроллере SDN-сети и позволяет выявлять нетипичное поведение сенсорных узлов и мобильных устройств пользователей. Пакеты выделяются парсером и передаются в анализатор. Модуль анализа извлекает характеристики пакета из заголовков протокольных блоков данных. Характеристики используются для кластеризации блоков данных в пространстве признаков с целью определения степени сходства с центроидами кластеров типичных и нетипичных пакетов, сформированных в процессе обучения нейронной сети. Кластеризация позволяет обнаружить факты модификации заголовков пакетов данных и компрометации сенсорных узлов. Для наборов характеристик нетипичных пакетов контроллер создает правила фильтрации в таблицах потоков, а для нормальных пакетов – правила ретрансляции.

Метод кластеризации пакетов реализован комбинированным способом с использованием аппарата нечеткой логики и нейронной сети. Примером такого подхода является технология обнаружения вторжений в системе ANFIS (Adaptive Network-based Fuzzy Inference System) [19]. Для синтеза пространства признаков и кластеризации в нем предлагается использовать девять характеристик, извлекаемых из заголовков IP пакетов и TCP сегментов, а именно IP-адрес источника (IP_src), IP-адрес назначения (IP_Dst), длину заголовка (Head_Lng), полную длину пакета (Total_Lng), идентификатор фрагмента (Frag_Id), время жизни пакета (TTL), тип сервиса (Srv_ type), номера портов протокола отправителя (Port_Srv) и получателя (Port_Dst). Начальное обучение нейронной сети выполняется на основе наборов характеристик пакетов от неавторизованных узлов, а в дальнейшем для обучения используются выявленные наборы характеристик нетипичных пакетов. Параметры функции принадлежности пакетов к кластерам настраиваются посредством алгоритма обучения нейронных сетей, а вывод о принадлежности и степени сходства с центроидами кластеров формируется с помощью аппарата нечеткой логики.

Метод нечеткой кластеризации базируется на алгоритме fuzzy c-means [20] и включает следующие шаги:

1. Задается число кластеров пакетов M, которое далее корректируется в процессе обучения, выбирается степень нечеткости целевой функции $m > 1$.

2. Входные наборы характеристик пакета представляют вектора признаков X_j (j = 1, …, N). Вектор определяет точку в пространстве, которая может относиться к кластерам с центроидами $C^{(k)}$ (k = 1, ..., M) и вероятностной функцией принадлежности $\mu_{X_j}^{(k)}$, где $0 < \mu_{X_j}^{(k)} < 1$, $\sum_{k=1}^{M} \mu_{X_j}^{(k)} = 1$, которая выступает в качестве степени сходства с центроидом и определяется как расстояние $D_{X_j}^{(k)}$.

3. Точки случайным образом распределяются по кластерам. Распределение точек определяется матрицей степеней сходства с центроидами в пространстве признаков с девятью координатами (x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}, x_{i6}, x_{i7}, x_{i8}, x_{i9}).

4. Вычисляются координаты центроидов кластеров C^k (k = 1, …, M) посредством вычисления средней близости точек кластера:

$$C_k = \frac{\sum_{k=1}^{M} \left(\mu_{X_j}^{(k)} X_j \right)}{\sum_{k=1}^{M} \left(\mu_{X_j}^{(k)} \right)}. \quad (1)$$

5. Определяются расстояния между точками и центроидами кластеров:

$$D_{X_j}^{(k)} = \sqrt{|| X_j - C^{(k)} ||^2}. \quad (2)$$

6. Пересчитываются степени принадлежности точек к кластерам и обновляется матрица распределения точек:

$$\mu_{X_j}^{(k)} = \frac{1}{\sum_{k=1}^{M} \left(\frac{D_{X_i}^{(k)}}{D_{X_j}^{(k)}} \right)^{2/m-1}}), \quad (3)$$

где $m > 1$ – коэффициент нечеткости кластеризации.

7. Для остановки итерационного процесса задается параметр $\varepsilon > 0$. Если условие $\{|\mu_{X_j}^{(k)} - \mu_{X_j}^{(k-1)}|\} < \varepsilon$ не выполняется, то производится переход к пункту 5.

Процедура обучения метода кластеризации реализуется посредством нейронной сети, которая представляет пятислойную структуру без обратных связей с весовыми коэффициентами и функциями активации (рис. 2). В качестве основы выбрана модель адаптивного типа Такаги – Сугено – Канга (TSK) [21]. Выходной сигнал определяется функцией агрегирования для M правил и N переменных (в нашем случае на входе сети N = 9 характеристик пакетов):

$$y(x) = \frac{\sum_{k=1}^{M} \left(w_k * y_k(x) \right)}{\sum_{k=1}^{M} \left(w_k \right)}, \quad (4)$$

где $y_k(x) = z_{k0} \sum_{j=1}^{N} \left(z_{kj} x_j \right)$ – i-й полиномиальный компонент аппроксимации, веса w_i представляют степень выполнения условий правила $w_k = \mu_A^{(\kappa)}(x_j)$.

Функция принадлежности или фуззификации $\mu_A^{(k)}$ для переменной x_j представляется функцией Гаусса

$$w_k = \mu_A^{(k)}(x_j) = \prod_{j=1}^{N} \left[\frac{1}{1 + \left(\frac{\left(x_j - c_j^{(k)} \right)}{\sigma_j^{(k)}} \right)^{2b_j^{(k)}}} \right], \qquad (5)$$

где k – количество функций принадлежности ($k = 1 \ldots M$); j – количество переменных ($N = 9$); $c_j^{(k)}, \sigma_j^{(k)}, b_j^{(k)}$ – параметры функции Гаусса, определяющие ее центр, ширину и форму k-й функции принадлежности j-й переменной.

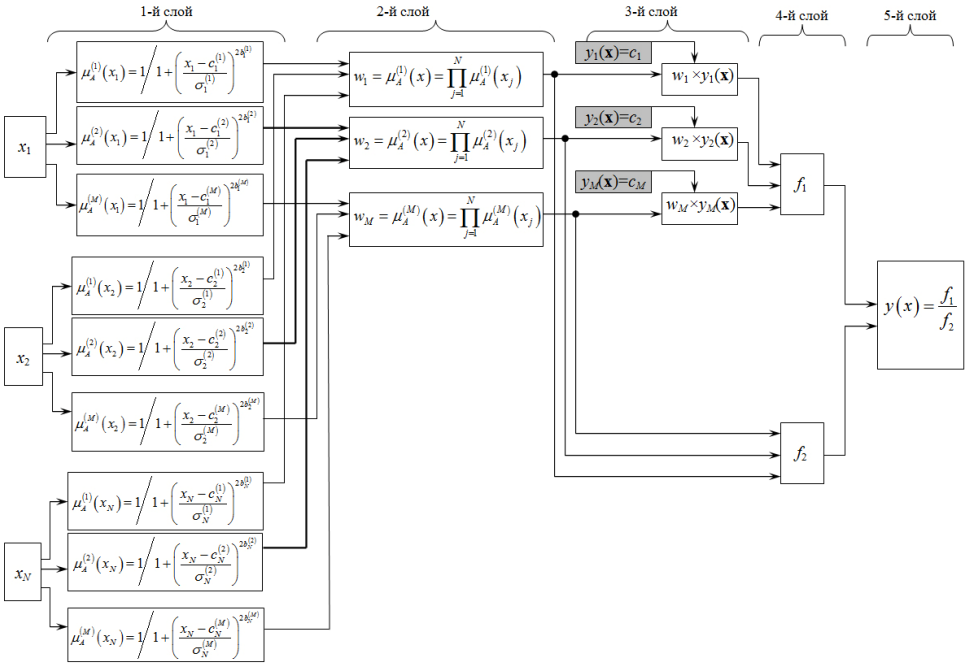

Рис. 2. Архитектура нечеткой нейронной сети
для кластеризации пакетов сетевого трафика

Правила вывода выходных переменных $Y = (y_1, y_2, \ldots, y_M)$ для множества переменных $X = (x_1, x_2, \ldots, x_9)$, принимающих множество значений $A_j^{(k)}$, представляет матрицу значений функций принадлежности размера $9 \times M$:

R_1: если $x_1^{(1)} \in A_1^{(1)}$ и $x_2^{(1)} \in A_2^{(1)}$ и, …, и $x_9^{(1)} \in A_9^{(1)}$, то $y_1(x) = z_{10} \sum_{j=1}^{9} (z_{1j} x_j)$,

… … … … (6)

R_M: если $x_1^{(M)} \in A_1^{(M)}$ и $x_2^{(M)} \in A_2^{(M)}$ и, …, и $x_9^{(M)} \in A_9^{(M)}$, то $y_M(x) = z_{M0} \sum_{j=1}^{9} (z_{Mj} x_j)$.

Для снижения вычислительной сложности допустим, что количество правил совпадает с количеством функций принадлежности, хотя они могут отличаться.

В первом слое осуществляется фуззификация согласно формуле (5) для каждой переменной x_i. При этом для каждого правила R_j определяются значения функции принадлежности $\mu_A^{(k)}(x_i)$:

$$\mu_A^{(k)}(x_j) = \frac{1}{1+\left(\frac{x_j - c_i^{(k)}}{\sigma_i^{(k)}}\right)^{2b_i^{(k)}}}. \quad (7)$$

Во втором слое определяются коэффициенты $w_{k=}\ \mu_A^{(k)}(x)$ путем агрегирования значений переменных x_i. Коэффициенты w_k передаются в 3-й слой, где умножаются на значения $y_i(x)$, а также в четвертый слой для вычисления суммы весов.

На третьем слое рассчитываются значения $y_i(x) = z_{k0}\sum_{j=1}^{N}\left(z_{kj} * x_j\right)$, которые умножаются на весовые коэффициенты w_k. Линейные параметры z_{k0} и z_{kj} являются функциями следствий правил, а z_{k0} рассматривается как центр функции принадлежности.

Четвертый слой представлен двумя нейронами (f_1 и f_2), выполняющими агрегирование результатов:

$$f_1 = \sum_{k=1}^{M} w_k y_k(\boldsymbol{x}) = \sum_{k=1}^{M}\left[\left(\prod_{j=1}^{N}\mu_A^{(k)}(x_j)\right)c_k\right], \quad (8)$$

$$f_2 = \sum_{k=1}^{M} w_k = \sum_{k=1}^{M}\left[\prod_{j=1}^{N}\mu_A^{(k)}(x_j)\right]. \quad (9)$$

Пятый нормализующий слой представлен одним нейроном, где веса подвергаются нормализации и вычисляется выходная функция:

$$y(x) = \frac{f_1}{f_2} = \frac{\sum_{k=1}^{M} w_k \times y_k(\boldsymbol{x})}{\sum_{k=1}^{M} w_k} = \frac{\sum_{k=1}^{M}\left[\left(\prod_{j=1}^{N}\mu_A^{(k)}(x_j)\right)\cdot c_k\right]}{\sum_{k=1}^{M}\left[\prod_{j=1}^{N}\mu_A^{(k)}(x_j)\right]}. \quad (10)$$

Значения параметров для первого и третьего слоя подбираются на этапе обучения. Параметры первого слоя $c_j^{(k)}, \sigma_j^{(k)}, b_j^{(k)}$ считаются нелинейными, а параметры третьего слоя z_{kj} – линейными. Обучение выполняется в два шага. На первом шаге подбираются параметры функций принадлежности третьего слоя посредством фиксации отдельных значений параметров и решения системы линейных уравнений

$$y(x) = \sum_{k=1}^{M} w_k\left(z_{k0} + \sum_{j=1}^{N}\left(z_{kj}x_j\right)\right). \quad (11)$$

Выходные переменные заменяются эталонными значениями d_P (P – число обучающих выборок). Систему уравнений можно записать в матричном виде: $D_P = W*Z$. Решение системы уравнений находится посредством

псевдоинверсной матрицы W^+: $Z = W^+D_P$. Далее после фиксации значений линейных параметров z_{kj} рассчитывается вектор Y фактических выходных переменных и определяется вектор ошибки $E = Y – D_P$.

На втором шаге ошибки направляются в обратном направлении до первого слоя, где рассчитываются параметры вектора градиента целевой функции принадлежности относительно параметров $c_j^{(k)}, \sigma_j^{(k)}, b_j^{(k)}$. Затем выполняется корректировка параметров функций принадлежности методом быстрого спуска по градиентному методу:

$$c_j^{(k)}(n+1) = c_j^{(k)}(n) - \eta \frac{\partial E(n)}{\partial c_j^{(k)}}, \quad (12)$$

$$\sigma_j^{(k)}(n+1) = \sigma_j^{(k)}(n) - \eta \frac{\partial E(n)}{\partial c_j^{(k)}}, \quad (13)$$

$$b_j^{(k)}(n+1) = b_j^{(k)}(n) - \eta \frac{\partial E(n)}{\partial b_j^{(k)}}, \quad (14)$$

где n – номер итерации; η – параметр скорости обучения.

После уточнения нелинейных параметров снова запускается процесс адаптации линейных и нелинейных параметров. Итерационный процесс повторяется, пока не стабилизируются все параметры процесса.

Для оценки вероятностной принадлежности пакета данных к кластерам нормальных и нетипичных пакетов применяется распределение степени принадлежности по трем интервалам:

а) 0–33 (%);

б) 34–66 (%);

в) 67–100 (%).

Решение о синтезе правил фильтрации принимается при попадании пакета в третий интервал. Такой пакет считается нетипичным, источник идентифицируется как скомпрометированный узел и его адрес добавляется в исключающее правило таблицы потоков. Если пакет попадает в первый интервал, то он считается нормальным. Создается правило для ретрансляции пакетов с аналогичными наборами характеристик и адрес источника добавляется в белый список. Попадание пакета во второй интервал означает, что его степень близости к кластерам нормальных и нетипичных пакетов под вопросом. Точка, соответствующая вектору признаков такого пакета, становится центроидом нового кластера. Число кластеров увеличивается на единицу, и повторно решается задача кластеризации. Результатом интеллектуального анализа пакетов данных является синтез правил их фильтрации/ретрансляции в коммутаторах, включение адресов источников в белый или черный списки, добавление записей в журнал событий безопасности, которые включают идентификатор скомпрометированного узла, IP-адрес, время обнаружения атаки, время фиксации события, тип транзакции и т.д.

Результаты

Разработана подсистема интеллектуального анализа и кластеризации, которая включает модули валидации сетевых узлов, фильтрации трафика,

журнализации, парсер и анализатор пакетов на базе нечеткой логики и нейронной сети, входящая в состав системы защищенного мониторинга критических событий в дорожно-транспортной инфраструктуре (рис. 3).

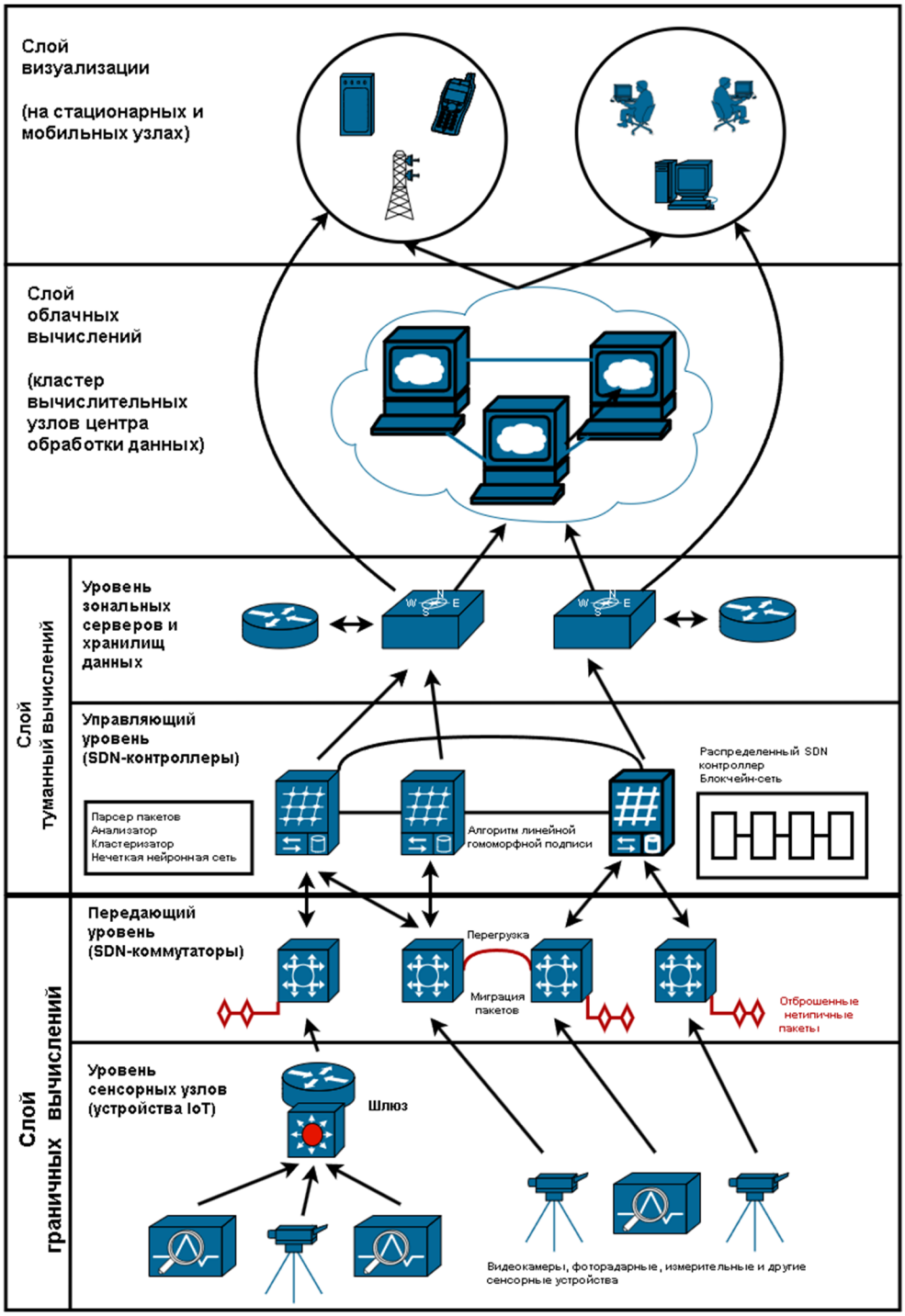

Рис. 3. Архитектура защищенной системы мониторинга

Система включает четыре слоя с шестью уровнями управления данными:

1) слой граничных вычислений, включающий уровень оконечных сенсорных узлов, маршрутизаторов, координаторов сенсорных сетей и уровень данных в SDN-коммутаторах. В слое реализуются процессы сбора, обработки и хранения телеметрических показателей работы оборудования и сенсорных данных, а функция ретрансляции/фильтрация пакетов в SDN-коммутаторах согласно правилам таблиц потоков;

2) слой туманных вычислений, включающий уровень зональных серверов и уровень управления в SDN-контроллерах. Слой реализует процедуры синтеза правил таблиц потоков, валидации цифровой подписи сетевых узлов, анализа и фильтрации сетевого трафика, обнаружения нетипичных пакетов на основе анализа заголовков и кластеризации, обучения нейронной сети, журналирования. В зональных серверах выполняются функции консолидации данных, агрегирования и хранения данных на основе технологии распределенной хеш-таблицы (Distributed Hash Table, DHT), так как основная часть данных является фотографиями или видеороликами с места инцидента, что решает проблему масштабируемости хранилища;

3) слой облачных вычислений на серверах центра обработки данных, который реализует основной функционал системы мониторинга по обработке и предиктивному анализу данных, централизованному хранению результатов;

4) слой визуализации предназначен для представления результатов мониторинга на мобильных и стационарных пользовательских устройствах.

Моделирование работы сетевой архитектуры системы мониторинга выполнено в системе Network Simulator версии 3 (NS3) [22, 23]. Для оценки эффективности анализа пакетов создано несколько неавторизованных узлов, которые генерируют нетипичные пакеты. Результатом моделирования являются оценки показателей работы архитектуры, такие как задержка передачи, время реакции, пропускная способность и точность распознавания пакетов. Оценка роста задержки передачи проведена в зависимости от увеличения числа сенсорных узлов и количества обрабатываемых пакетов (рис. 4).

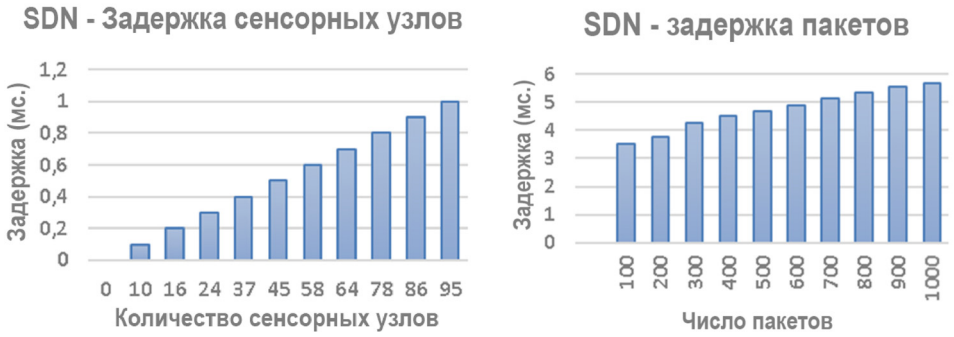

Рис. 4. Диаграммы зависимости задержки от числа сенсорных узлов и числа пакетов

Графики показывают, что величина задержки увеличивается по мере увеличения количества устройств с изменениями нескольких миллисекунд после передачи пакета от конечного узла. Однако при увеличении числа узлов

задержка становится существенной, так как наблюдается линейная зависимость.

Время реакции определяется на основе запросов, поступивших от конечных узлов к шлюзу, которые передаются на коммутаторы, где выполняется их ретрансляция или фильтрация после анализа пакетов. Сравнение времени реакции в предлагаемой архитектуре со временем реакции в традиционной архитектуре без анализа и кластеризации показало увеличение задержки в среднем на 10,5 % (рис. 5).

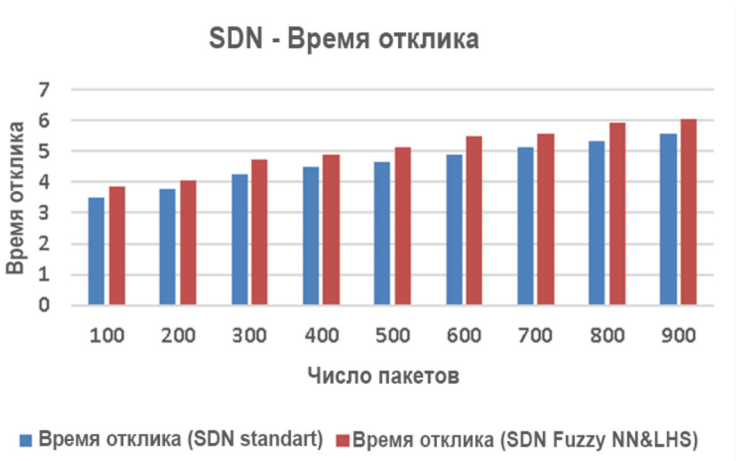

Рис. 5. Сравнение времени реакции сети с традиционной SDN-архитектурой и сети с подсистемой анализа и кластеризации

На рис. 6 приводятся диаграммы изменения пропускной способности в зависимости от числа запросов к узлам сети. Снижение пропускной способности в среднем до 16 % в предлагаемой архитектуре происходит из-за затрат времени на анализ, распознавание и кластеризацию пакетов.

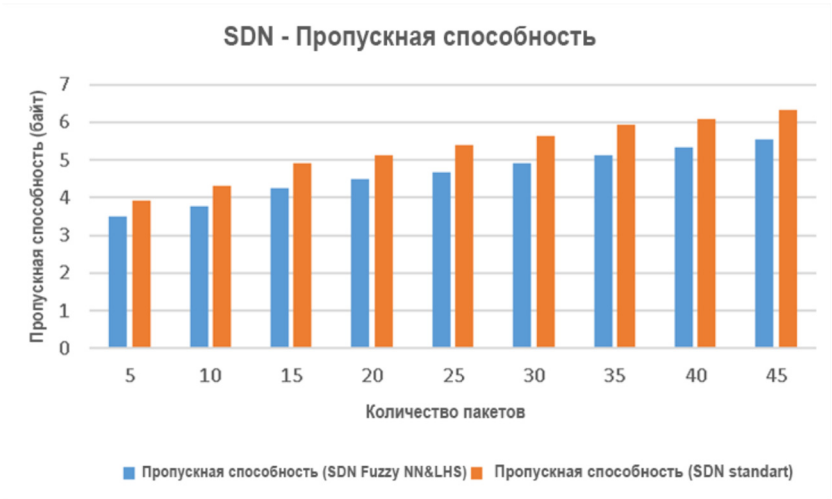

Рис. 6. Сравнение пропускной способности в сетях с традиционной и предлагаемой архитектурой

Для оценки эффективности предлагаемого подхода используется оценка точности распознавания нетипичных пакетов. В табл. 1 показана точность обнаружения нетипичных пакетов в зависимости от скорости поступления коммутаторов. Точность обнаружения достаточно высока, но снижается по мере роста скорости поступления пакетов, что обусловлено временем анализа пакетов и синтеза правил таблиц потоков.

Таблица 1

Точность обнаружения нетипичных пакетов

Поступающие на обработку пакеты (пакет/сек)	Общее число пакетов		Число пакетов в результате кластеризации		Точность распознавания (%)
	Нормальные пакеты	Нетипичные пакеты	Нормальные пакеты	Нетипичные пакеты	
20	400	75	399	76	98,68
40	800	150	797	153	98,03
60	1200	225	1195	230	97,82
80	1600	300	1590	310	96,77
100	2000	375	1980	395	94,94

Обсуждение

Развитие технологий IoT, распределенного реестра и программно-конфигурируемых сетей привело росту исследований в направлении их интеграции. В статье представлена архитектура защищенной системы распределенного мониторинга, реализующая технологию интеллектуального управления трафиком. Аналогичная архитектура рассматривается в статье [25], основным отличием которой является трехуровневая модель транспортной среды, включающей уровень коммутаторов, контроллеров и облачный уровень для реализации технологии блокчейн для защиты блоков данных. В нашей архитектуре технология хранения блоков данных в виде распределенного реестра реализована на зональных серверах туманного слоя. Задачи фильтрации трафика, валидации узлов, анализа и распознавания пакетов решаются на уровне коммутаторов краевого слоя и уровне контроллеров туманного слоя обработки данных. Интеграция зональных серверов и SDN-контроллеров на туманном слое вычислений позволяет перераспределить нагрузку для масштабирования, а также разделить процессы защиты данных от их обработки и хранения. Сервера облачного слоя решают задачи статистического и предиктивного анализа консолидированных сенсорных данных после их предварительной обработки и агрегирования на зональных серверах.

Другим примером синтеза защищенной транспортной среды для мониторинга дорожной инфраструктуры являются результаты исследований в работе [24]. Здесь рассмотрены вопросы синтеза системы связи автомобильных контроллеров и блоков управления. Авторы предлагают использовать технологию SDN-сети с блокчейном для обеспечения конфиденциальности данных производителей и владельцев автотранспорта с целью обнаружения несанкционированного доступа к системе управления автомобилем. Авторы статьи [6] исследуют преимущества интеграции блокчейна и SDN в одноранговых сетях IoT на основе предложенного протокола маршрутизации с решением задачи

кластеризации узлов для оптимизации энергопотребления. В работе [7] авторы предлагают децентрализованную архитектуру SDN-сети на основе блокчейна для «умного» города, которая предназначена для сбора данных и защиты от киберугроз. В нашем случае архитектура защищенной системы мониторинга разработана для применения в дорожно-транспортной инфраструктуре. Преимуществом предлагаемого подхода является комбинированный метод анализа пакетов атак на основе пятислойной нейронной сети с технологией глубокого обучения и методики оценки вероятностной принадлежности пакетов к нормальным и нетипичным блокам на основе нечеткой логики.

Для решения проблемы уязвимости при передаче данных между плоскостью управления и плоскостью данных архитектуры SDN-сети в работе [25] предлагается использование стороннего сервиса для проверки потоков за вознаграждение. Однако данный подход не может применяться для обеспечения безопасности в системах «Безопасный город» и «Безопасная дорога». Во-первых, это увеличивает стоимость услуг, во-вторых, делегирует ответственность за проблемы с безопасностью третьим лицам и, в-третьих, усложняет и замедляет процесс обнаружения киберугроз [26, 27]. В статье [28] для решения проблемы безопасного доступа авторы предлагают в качестве механизма авторизации использовать блокчейн и атрибутивное шифрование, что увеличивает время реакции системы. В нашем случае преимуществом является снижение вычислительной нагрузки на контроллеры за счет трехступенчатой технологии анализа сетевого трафика. На первом этапе выполняется фильтрация трафика по номерам портов. На втором этапе подтверждается подлинность источников данных и устройств доступа с целью фильтрации трафика от недопустимых узлов из «черного» списка. На третий этап, где выполняются затратные по времени процедуры анализа и распознавания, допускается ограниченное число отфильтрованных пакетов.

Основной проблемой большинства традиционных сенсорных сетей являются ограничения по пропускной способности каналов связи и вычислительным ресурсам сенсорных узлов [29]. Ограничения не позволяют решать задачи большой вычислительной сложности по использованию технологий блокчейна для обеспечения безопасности непосредственно на сенсорных узлах. В системе мониторинга дорожно-транспортной инфраструктуры сенсорными узлами являются фоторадарные комплексы и камеры видеонаблюдения, работающие в рамках стандартов беспроводных сетей WiFi, WiGi (802.11) и мобильных сетей 4G с каналами связи достаточно высокой пропускной способности. В связи с этим особых ограничений, связанных с пропускной способностью каналов передачи данных в предложенной архитектуре, практически нет. Для решения проблемы ресурсных ограничений основные вычислительные задачи решаются на уровне зональных и облачных серверов. Еще одна проблема связана с масштабируемостью программно-конфигурируемой сети [11]. Она возникает при централизации в SDN-контроллере процессов управления трафиком и усиливается при добавлении новых функций валидации узлов, анализа трафика и кластеризации пакетов. Способом решения проблемы является использование нескольких контроллеров с гипервизором для балансировки трафика и перераспределения пакетов, поступающих для анализа и обнаружения атак.

Заключение

В ходе исследований синтезирована безопасная архитектура системы дорожно-транспортного мониторинга с использованием технологии SDN-сетей, распределенного реестра, анализа и кластеризации пакетов данных с использованием нечеткой нейронной сети. В работе представлен ряд результатов:

а) SDN-архитектура системы с четырьмя слоями устройств и шестью уровнями управления данными;

б) метод обнаружения кибератак с использованием нечеткой нейронной сети и алгоритма кластеризации для оценки пакетов по девяти характеристикам;

в) набор характеристик пакетов данных для распознавания и вероятностной оценки вредоносных пакетов.

Моделирование и оценка эффективности предложенного подхода показала достаточно высокую скорость обработки трафика в системе мониторинга. Для снижения вычислительной нагрузки реализована трехступенчатая технология анализа. На первом этапе выполняется фильтрация недопустимого трафика по номерам портов. На втором этапе подтверждается подлинность источников данных и устройств доступа и фильтруется трафик от недопустимых узлов. На третьем этапе выполняются процедуры машинного обучения и интеллектуального анализа отфильтрованных пакетов.

Список литературы

1. Finogeev A., Finogeev A. Information attacks and security in wireless sensor networks of industrial SCADA systems // Journal of Industrial Information Integration. 2017. Vol. 5. P. 6–16. doi: 10.1016/j.jii.2017.02.002
2. Zaman S., Alhazmi K., Aseeri M. A. [et al.]. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey // Access IEEE. 2021. Vol. 9. P. 94668–94690.
3. Contia M., Dehghantanhab A., Frankec K., Watsond S. Internet of Things security and forensics: Challenges and opportunities // Future Generation Computer Systems. 2018. Vol. 78, part 2. P. 544–546.
4. Finogeev A., Finogeev A., Shevchenko S. Monitoring of Road Transport Infrastructure for the Intelligent Environment «Smart Road», Communications // Computer and Information Science. 2017. Vol. 754. P. 655–668. doi: 10.1007/978-3-319-65551-2_47
5. Finogeev A., Deev M., Finogeev A., Kolesnikoff I. Proactive Big Data Analysis for Traffic Accident Prediction // Proceeding of the 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA). 2020. doi: 10.1109/CITISIA50690.2020.9371796
6. Latif S. A., Wen F. B. X., Iwendi C. [et al.]. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systemsm // Computer Communication. 2022. Vol. 181. P. 274–283.
7. Islam Md., Rahman A., Kabir S. [et al.]. Blockchain-SDN based Energy-Aware and Distributed Secure Architecture for IoTs in Smart Cities // IEEE Internet of Things Journal. 2021. Vol. 9. P. 3850–3864. doi: 10.1109/JIOT.2021.3100797
8. Mousavi S. M. Early Detection of DDoS Attacks in Software Defined Networks Controller. Ontario : Carleton University Ottawa, 2014.
9. Yan Q., Yu F. R. Distributed denial of service attacks in software-defined networking with cloud computing // IEEE Communications Magazine. 2015. Vol. 53, iss. 4. P. 52–59.
10. Zhu L., Karim Md. M., Sharif K. [et al.]. SDN Controllers // ACM Computing Surveys. 2021. Vol. 53. P. 1.

11. Hassas Y. S., Tootoonchian A., Ganjali Y. On scalability of software-defined networking // IEEE Communications Magazine. 2013. Vol. 51. P. 136–141.
12. Valdovinos I. A., Pérez-Díaz J. A., Choo K.-K. R., Botero J. F. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy challenges and future directions // Journal of Network and Computer Applications. 2021. Vol. 187. P. 103093.
13. Alam I., Sharif K., Li F. [et al.]. A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV // ACM Computing Surveys. 2021. Vol. 53. P. 1.
14. Bawany N. Z., Shamsi J. A., Salah K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions // Arabian Journal for Science and Engineering. 2017. Vol. 42. P. 425–441. doi: 10.1007/s13369-017-2414-5
15. Mohamed M. B., Alofe O. M., Azad M. A. [et al.]. A comprehensive survey on secure software-defined network for the Internet of Things // Transactions on Emerging Telecommunications Technologies. 2022. Vol. 33.
16. Giri N., Jaisinghani R., Kriplani R. [et al.]. Distributed Denial Of Service (DDoS) Mitigation in Software Defined Network using Blockchain // IoT in Social Mobile Analytics and Cloud (I-SMAC). 2019. P. 673–678.
17. Lee C. H., Kim K.-H. Implementation of IoT system using block chain with authentication and data protection // Proceedings of International Conference on Information Networking (ICOIN). 2018. P. 936–940.
18. Velmurugadass P., Dhanasekaran S., Shasi Anand S., Vasudevan V. Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm // Materials Today : proceedings. 2021. Vol. 37. P. 2653.
19. Jang J.-S. R. ANFIS: adaptive-network-based fuzzy inference system // IEEE Transactions on Systems, Man and Cybernetics. 1993. Vol. 23, № 3. P. 665–685.
20. Khang T. D., Vuong N. D., Tran M.-K., Fowler M. Fuzzy C-Means Clustering Algorithm with Multiple Fuzzification Coefficients // Algorithms. 2020. Vol. 13. P. 158. doi: 10.3390/a13070158
21. Chang P. C., Liu C. H. A TSK Type Fuzzy Rule Based System for Stock Price Prediction // Expert Systems with Applications. 2008. Vol. 34, № 1. P. 135–144.
22. Network Simulator ns-3. URL: https://www.nsnam.org/releases/ns-3-35/ (дата обращения: 12.05.2023).
23. Lavacca F. G., Salvo P., Ferranti L. [et al.]. Performance Evaluation of 5G Access Technologies and SDN Transport Network on an NS3 Simulator // Computers. 2020. Vol. 9. P. 43. doi: 10.3390/computers9020043
24. Aliyu I., Feliciano M. C., Van Engelenburg S. [et al.]. A Blockchain-Based Federated Forest for SDN-Enabled In-Vehicle Network Intrusion Detection System // IEEE Access. 2021. Vol. 9. P. 102593–102608. doi: 10.1109/ACCESS.2021.3094365
25. Sharma P. K., Chen M.-Y., Park J. H. A software defined fog node based distributed blockchain cloud architecture for IoT // IEEE Access. 2018. Vol. 6. P. 115–124.
26. Finogeev A., Finogeev A., Fionova L. [et al.]. Intelligent monitoring system for smart road environment // Journal of Industrial Information Integration. 2019. Vol. 15. P. 15–20. doi: 10.1016/j.jii.2019.05.003
27. Finogeev A., Parygin D., Schevchenko S. [et al.]. Collection and Consolidation of Big Data for Proactive Monitoring of Critical Events at Infrastructure Facilities in an Urban Environment // Creativity in Intelligent Technologies and Data Science (CIT&DS) Communications in Computer and Information Science 2021 / ed. by A. G. Kravets, M. Shcherbakov, D. Parygin, P. P. Groumpos. Springer, Cham., 2021. Vol 1448. doi: 10.1007/978-3-030-87034-8_25
28. Gelenbe E., Domanska J., Czàchorski T. [et al.]. Security for Internet of Things: The Seriot project // Proceedings of IEEE International Symposium on Networks, Computers and Communications (ISNCC). 2018. P. 1–5.

29. Ren W., Sun Y., Luo H., Guizani M. SILedger: A Blockchain and ABE-based Access Control for Applications in SDN-IoT Networks // IEEE Transactions on Network and Service Management. 2021. Vol. 18. P. 4406–4419. doi: 10.1109/TNSM.2021.3093002

References

1. Finogeev A., Finogeev A. Information attacks and security in wireless sensor networks of industrial SCADA systems. *Journal of Industrial Information Integration*. 2017;5:6–16. doi: 10.1016/j.jii.2017.02.002
2. Zaman S., Alhazmi K., Aseeri M. A. et al. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. *Access IEEE*. 2021;9:94668–94690.
3. Contia M., Dehghantanhab A., Frankec K., Watsond S. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*. 2018;78(part 2):544–546.
4. Finogeev A., Finogeev A., Shevchenko S. Monitoring of Road Transport Infrastructure for the Intelligent Environment «Smart Road», Communications. *Computer and Information Science*. 2017;754:655–668. doi: 10.1007/978-3-319-65551-2_47
5. Finogeev A., Deev M., Finogeev A., Kolesnikoff I. Proactive Big Data Analysis for Traffic Accident Prediction. *Proceeding of the 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*. 2020. doi: 10.1109/CITISIA50690.2020.9371796
6. Latif S. A., Wen F. B. X., Iwendi C. et al. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systemsm. *Computer Communication*. 2022;181:274–283.
7. Islam Md., Rahman A., Kabir S. et al. Blockchain-SDN based Energy-Aware and Distributed Secure Architecture for IoTs in Smart Cities. *IEEE Internet of Things Journal*. 2021;9:3850–3864. doi: 10.1109/JIOT.2021.3100797
8. Mousavi S.M. *Early Detection of DDoS Attacks in Software Defined Networks Controller*. Ontario: Carleton University Ottawa, 2014.
9. Yan Q., Yu F.R. Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Communications Magazine*. 2015;53(4):52–59.
10. Zhu L., Karim Md. M., Sharif K. et al. SDN Controllers. *ACM Computing Surveys*. 2021;53:1.
11. Hassas Y.S., Tootoonchian A., Ganjali Y. On scalability of software-defined networking. *IEEE Communications Magazine*. 2013;51:136–141.
12. Valdovinos I.A., Pérez-Díaz J.A., Choo K.-K.R., Botero J.F. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy challenges and future directions. *Journal of Network and Computer Applications*. 2021;187:103093.
13. Alam I., Sharif K., Li F. et al. A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV. *ACM Computing Surveys*. 2021;53:1.
14. Bawany N.Z., Shamsi J.A., Salah K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. *Arabian Journal for Science and Engineering*. 2017;42:425–441. doi: 10.1007/s13369-017-2414-5
15. Mohamed M.B., Alofe O.M., Azad M.A. et al. A comprehensive survey on secure software-defined network for the Internet of Things. *Transactions on Emerging Telecommunications Technologies*. 2022;33.
16. Giri N., Jaisinghani R., Kriplani R. et al. Distributed Denial Of Service (DDoS) Mitigation in Software Defined Network using Blockchain. *IoT in Social Mobile Analytics and Cloud (I-SMAC)*. 2019:673–678.
17. Lee C.H., Kim K.-H. Implementation of IoT system using block chain with authentication and data protection. *Proceedings of International Conference on Information Networking (ICOIN)*. 2018:936–940.

18. Velmurugadass P., Dhanasekaran S., Shasi Anand S., Vasudevan V. Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today : proceedings*. 2021;37:2653.
19. Jang J.-S.R. ANFIS: adaptive-network-based fuzzy inference system. *IEEE Transactions on Systems, Man and Cybernetics*. 1993;23(3):665–685.
20. Khang T.D., Vuong N.D., Tran M.-K., Fowler M. Fuzzy C-Means Clustering Algorithm with Multiple Fuzzification Coefficients. *Algorithms*. 2020;13:158. doi: 10.3390/a13070158
21. Chang P.C., Liu C.H. A TSK Type Fuzzy Rule Based System for Stock Price Prediction. *Expert Systems with Applications*. 2008;34(1):135–144.
22. *Network Simulator ns-3*. Available at: https://www.nsnam.org/releases/ns-3-35/ (accessed 12.05.2023).
23. Lavacca F.G., Salvo P., Ferranti L. et al. Performance Evaluation of 5G Access Technologies and SDN Transport Network on an NS3 Simulator. *Computers*. 2020;9:43. doi: 10.3390/computers9020043
24. Aliyu I., Feliciano M.C., Van Engelenburg S. et al. A Blockchain-Based Federated Forest for SDN-Enabled In-Vehicle Network Intrusion Detection System. *IEEE Access*. 2021;9:102593–102608. doi: 10.1109/ACCESS.2021.3094365
25. Sharma P.K., Chen M.-Y., Park J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access*. 2018;6:115–124.
26. Finogeev A., Finogeev A., Fionova L. et al. Intelligent monitoring system for smart road environment. *Journal of Industrial Information Integration*. 2019;15:15–20. doi: 10.1016/j.jii.2019.05.003
27. Finogeev A., Parygin D., Schevchenko S. et al. Collection and Consolidation of Big Data for Proactive Monitoring of Critical Events at Infrastructure Facilities in an Urban Environment. *Creativity in Intelligent Technologies and Data Science (CIT&DS) Communications in Computer and Information Science 2021*. Springer, Cham., 2021;1448. doi: 10.1007/978-3-030-87034-8_25
28. Gelenbe E., Domanska J., Czàchorski T. et al. Security for Internet of Things: The Seriot project. *Proceedings of IEEE International Symposium on Networks, Computers and Communications (ISNCC)*. 2018:1–5.
29. Ren W., Sun Y., Luo H., Guizani M. SILedger: A Blockchain and ABE-based Access Control for Applications in SDN-IoT Networks. *IEEE Transactions on Network and Service Management*. 2021;18:4406–4419. doi: 10.1109/TNSM.2021.3093002

Информация об авторах / Information about the authors

Антон Алексеевич Финогеев
кандидат технических наук,
доцент кафедры систем
автоматизированного проектирования,
Пензенский государственный университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: fanton3@yandex.ru

Anton A. Finogeev
Candidate of technical sciences,
associate professor of the sub-department
of computer-aided design systems,
Penza State University
(40 Krasnaya street, Penza, Russia)

Автор заявляет об отсутствии конфликта интересов /
The author declares no conflicts of interests.

Поступила в редакцию/Received 24.03.2023
Поступила после рецензирования/Revised 20.06.2023
Принята к публикации/Accepted 04.07.2023