СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

УДК 004.056.5, 004.8 Научная статья
DOI: 10.35330/1991-6639-2023-6-116-235-246
EDN: SPQSZQ

Модель интеллектуального распределения трафика в кластерных сегментах теплотехнологических систем*

Б. В. Окунев[1], Е. К. Верейкина[2], А. И. Лазарев[1]

[1]Национальный исследовательский университет
Московский энергетический институт – филиал в г. Смоленске
214013, Россия, г. Смоленск, Энергетический проезд, 1
[2]Национальный исследовательский университет
Московский энергетический институт
111250, Россия, Москва, Красноказарменная улица, 17

Аннотация. В настоящее время принятие решений по управлению теплотехнологическими системами является достаточно сложным процессом. Непосредственное расширение параметров и взаимосвязанных элементов между участниками существенно сказывается на масштабировании систем оценки и контроля потоков информации. Несмотря на достаточно стремительное развитие информационно-коммуникационных технологий, существующие инструменты организации инфраструктурной поддержки процессов взаимодействия между клиентом и сервером все еще имеют существенные недостатки. Несовершенство таких решений не только сдерживает возможности роста их эффективности, но и является уязвимостью с точки зрения безопасности функционирования системы в целом. Целью исследования является алгоритмическая и программная разработка гибкой топологии сегментов сети с учетом динамически изменяющихся факторов. В результате проведен анализ существующих решений построения модульных сетевых протоколов для организации функционирования сложных систем. Выявлены их сильные стороны, уязвимости и потенциальные источники роста эффективности, на развитие и устранение которых направлено разработанное решение. Построена модель безопасной сети удаленного взаимодействия и обмена критически важной информацией для обеспечения стабильной работы сложно-технического оборудования в теплотехнологической системе. Особенностью разработанной модели является модуль безопасного доступа к требуемой информации за счет прямого *p2p* обмена между клиентами при помощи безопасного туннеля. Практическая значимость заключается в возможности использования разработанной модели интеллектуального распределения трафика в сегментах сети теплотехнологических систем различных видов экономической деятельности.

Ключевые слова: TCP/IP топологии, обеспечение безопасности данных, управление данными, нейронные модели, теплотехнологические комплексы

Поступила 03.11.2023, одобрена после рецензирования 09.11.2023, принята к публикации 13.11.2023

Для цитирования. Окунев Б. В., Верейкина Е. К., Лазарев А. И. Модель интеллектуального распределения трафика в кластерных сегментах теплотехнологических систем // Известия Кабардино-Балкарского научного центра РАН. 2023. № 6(116). С. 235–246. DOI: 10.35330/1991-6639-2023-6-116-235-246

* Исследование выполнено за счет гранта Российского научного фонда (проект № 22-21-00487)

MSC: 68; 94 Original article

Intelligent traffic distribution model in cluster segments of heat technology systems*

B.V. Okunev[1], E.K. Vereykina[2], A.I. Lazarev[1]

[1]National Research University
Moscow Energy Institute – branch in Smolensk
214013, Russia, Smolensk, 1 Energeticheskiy proezd
[2]National Research University
Moscow Energy Institute
111250, Russia, Moscow, 17 Krasnokazarmennaya street

Abstract. Nowadays decision-making on the management of heat technology systems is a rather complex process. The parameters direct expansion and interrelated elements among participants significantly affects the scaling of information flow assessment and control systems. Despite the rather rapid information and communication technologies development, the existing tools for organizing infrastructure support for the processes of interaction between the client and the server still have significant drawbacks. The imperfection of such solutions not only hinders the increasing of their effectiveness possibility, but also are vulnerabilities from the point of the security system functioning view as a whole. The purpose of the study is algorithmic and software develop of network segments flexible topology taking into account dynamically changing factors. As a result, an analysis of existing solutions for the construction of modular network protocols for the organization of the functioning of complex systems is carried out. Their advantages, vulnerabilities and potential sources of efficiency growth have been identified, which the proposed solution is aimed at their improvement and elimination. A model of a secure network of remote interaction and exchange of critical information is built to ensure stable operation of complex technical equipment in a heat technology system. A special feature of the developed model is the module of secure access to the required information due to direct *p2p* exchange between clients using a secure tunnel. The practical significance lies in the possibility of using the developed model of intelligent traffic distribution in the network segments of heat technology systems of various types of economic activity.

Keywords: TCP/IP topologies, data security, data management, neural models, thermal technology complexes

Submitted 03.11.2023, approved after reviewing 09.11.2023, accepted for publication 13.11.2023

For citation. Okunev B.V., Vereykina E.K., Lazarev A.I. Intelligent traffic distribution model in cluster segments of heat technology systems. *News of the Kabardino-Balkarian Scientific Center of RAS.* 2023. No. 6(116). Pp. 235–246. DOI: 10.35330/1991-6639-2023-6-116-235-246

Введение

Усложнение теплотехнологических систем, связанное с увеличением числа вовлекаемых участников, их параметров и элементов, требующих оценки и контроля, а также кратный рост в связи с этим потоков информации и связей различного рода делают принятие решений по управлению ими в настоящее время достаточно сложным. Кроме того, отмечаемый курс на реализацию программ по импортозамещению, определяющий необходимость высокотехнологичных и немедленных производственных решений, обусловливает его актуальность. Поэтому системы мониторинга реализации производственных и бизнес-процессов, прежде всего в сфере использования возможностей тепловой энергии, выходят на первый план. Так как особенно сейчас инновационные решения по созданию

* The research was supported by a grant from the Russian Science Foundation (project No. 22-21-00487)

аналогов и рост эффективности в них являются неотъемлемой основой развития. Вместе с тем сложности, а зачастую практически невозможность влияния на факторы внешней среды, достоверно их оценивать и прогнозировать в связи с высоким динамизмом, изменчивостью и слабой предсказуемостью побуждают предприятия и организации искать источники повышения эффективности в рамках внутренних границ системы.

Несмотря на достаточно стремительное развитие информационно-коммуникационных технологий сейчас и их активное использование как средств коммуникаций, обмена, мониторинга и оценки, некоторые из существующих инструментов организации инфраструктурной поддержки процессов взаимодействия между клиентом и сервером все еще имеют существенные недостатки, которые не только сдерживают возможности роста их эффективности, но и являются уязвимостями с точки зрения безопасности функционирования системы в целом. Для теплотехнологических систем этот аспект является критически важным.

Для устранения данных недостатков было предложено разработать уникальную систему первичной инициализации безопасного соединения между отдельными клиентами теплотехнологического комплекса, а также обеспечить поддержку безопасности работы через виртуальный туннель. При реализации такой модели предлагается использовать универсальную топологию *IP*-сегментации устройств и прогнозное определение нагрузок трафика клиентов для поддержки безопасного обмена данными. Одной из главных особенностей разработанного решения является интеллектуальный выбор метода передачи с поддержкой *p2p*-соединения с клиентами, что позволит в дальнейшем расширять область его применения в узкоспециализированных сетевых топологиях, в том числе на промышленных установках для поддержки работы критически важной инфраструктуры.

Анализ существующих решений построения модульных сетевых протоколов для организации функционирования сложных систем

Обмен информацией между субсистемами сложных теплотехнологических комплексов может осуществляться как в рамках взаимодействия с сервером, так и через технологии *peer-to-peer (p2p)* передачи данных между клиентами [1]. Для автоматизации обмена информацией используются различные программно-аппаратные средства, включая протоколы передачи данных и удаленный доступ к комплексам через *VPN*-туннель. Однако эти инструменты не всегда удовлетворяют требованиям безопасности, особенно когда речь идет о передаче критически важных данных. Несанкционированное изменение таких данных может привести к серьезным проблемам на производстве.

На данный момент распространенной топологией взаимодействия между организациями является *TCP/IP* топология, основанная на типизированной работе серверного оборудования с наличием *DHCP*-сервера для назначения адресов клиентам. Однако ее нельзя интегрировать в теплотехнологические комплексы из-за ряда недостатков, среди которых можно выделить сложность отслеживания трафика клиентов с привязкой к реальному идентификатору. Кроме того, стандартизированный *DHCP*-сервер имеет относительно сложную систему назначения прав сервера клиентам для поддержки гибкой кластеризации данных. *DHCP*-сервер поддерживает статичное назначение адресов клиентам сети. Однако для организаций с частичным/полным аутсорсингом сотрудников использование статичного пула IP-адресов не является целесообразным.

Рассматривая *TCP/IP* технологию, можно отметить, что ее многогранное ветвление поддерживает работу в беспроводном режиме *WiFi* 4/5/6 на большинстве портативных

устройств. В среднечисленных масштабах организации часто используется топология, состоящая из роутера с наличием усилителей в удаленных дислокациях сетевых розеток [2]. Однако на сегодняшний день более адаптивная реализация такой топологии возможна благодаря использованию *mesh*-сетей. Эти сети позволяют в беспроводном режиме создавать сегмент сети, ограниченный лишь радиусом действия *mesh*-клиентов [3].

Mesh-системы представляют собой инновационную децентрализованную сеть, где каждое устройство имеет одинаковые права на доступ в интернет, функционируя как клиент и сервер одновременно. Такая топология является универсальным способом распределения интернет-доступа для различных устройств, включая *IoT*-оборудование [4]. Кроме того, использование *mesh*-системы обеспечивает возможность сегментации сети на отдельные участки с выделенным пулом *IP*-адресов [5]. Также необходимо отметить отсутствие необходимости в использовании дополнительного специализированного аппаратного оборудования для сети данного вида.

После настройки соединения и создания нескольких сегментов сети важным шагом в обеспечении стабильной передачи данных между участниками теплотехнических систем является этап оптимизации нагрузки трафика. Существующие программные решения для повышения эффективности в данной области, такие как технология *IntelliQoS* от *Keenetic*, позволяют определять приоритетность для распределения трафика с помощью классификации сервисов (например, голосовых вызовов, интернета вещей). Другое технологическое решение – *Quality of Service (QoS)* – используется в устройствах *Cisco*. *QoS* использует систему запросов и ответов для выбора полосы пропускания трафика [6–8]. Хотя эти инструменты могут решить проблему неравномерного распределения трафика, сетевое оборудование должно иметь приоритет перед другими устройствами или быть центральным устройством в топологии. В других случаях, когда управление устройствами в различных сегментах сети осуществляется с помощью различного сетевого оборудования, проблема централизованного распределения трафика остается актуальной.

Разработанная интеллектуальная модель взаимодействия участников сложных теплотехнологических систем в виде многоуровневой структуры сети

Разработанная гибкая система взаимоотношений при инициализации туннеля между клиентами теплотехнологического комплекса показана на рисунке 1. Каждый клиент такой сети в различные периоды времени и в зависимости от решаемых задач может выступать сервером для другого сегмента сети клиентов. Ее структура базируется на использовании *mesh*-топологии, которая даст возможность реализовать такую же гибкость, как при наличии специализированных аппаратных устройств, но без его реального использования.

На первоначальном этапе назначения адресов планируется инициализация *DHCP*-сервера на базе пакета *isc-dhcp-server* с использованием технологии выделения виртуальных мешей [9, 10]. Субмодуль первичного объединения устройств выполняет лимитирование доступного сегмента, что приводит к выделению нового меша для сегмента устройств. Таким образом, первоначальный меш из двух устройств контролирует сервер ID_0, а ID_1 – клиент. В новом меше клиент ID_1 становится сервером для меша № 1. В данном случае для принятия решений используются два модуля, а именно: процесс нечеткого посимвольного сравнения и изменчивость потока данных. Процесс нечеткого посимвольного сравнения в данном случае работает как цифровой идентификатор, который используется для проверки подлинности устройства. Этот подход позволяет использовать только один программный модуль и минимизировать использование аппаратных ресурсов устройств в сети.

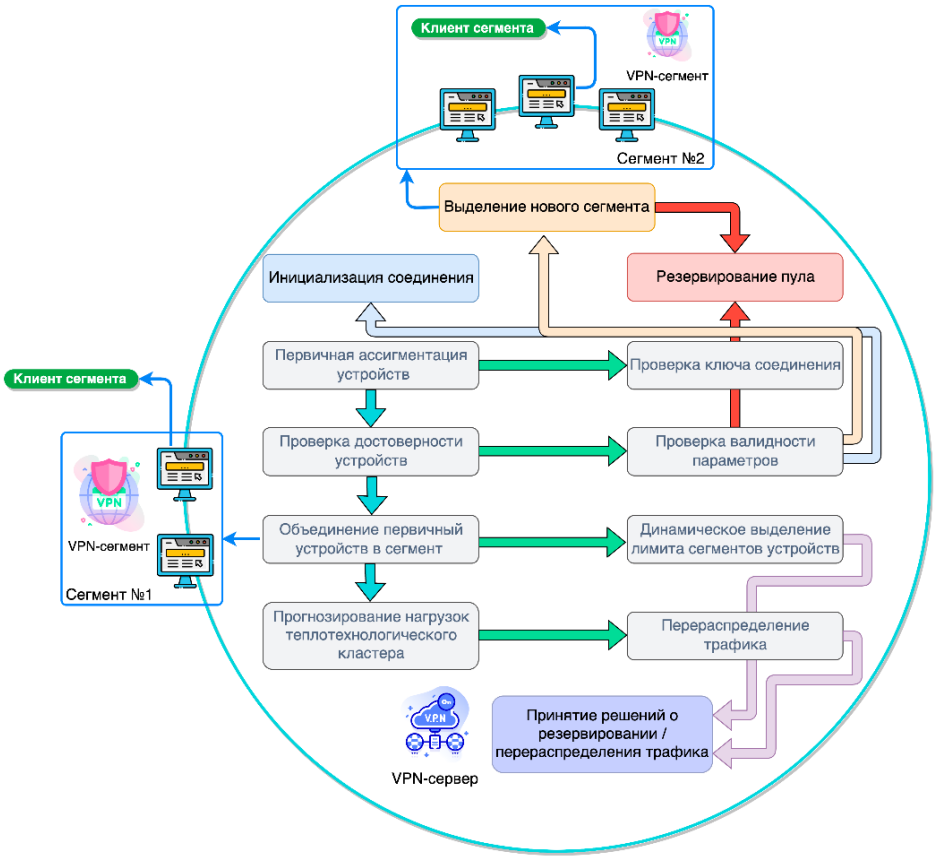

Рис. 1. *Алгоритм меш-инициализации виртуальной топологии VPN-туннелирования*

Fig. 1. *Algorithm for mesh initialization of virtual VPN tunneling topology*

На этапе идентификации первичных параметров асигментации устройств устанавливаются два автономных агента, которые работают как сервер и клиент для поиска совместимых элементов меша. Для первоначального назначения устройств используется модуль генерации уникального временного *TOTP-AUTH* кода, который использует статический идентификатор аппаратной составляющей устройства и системное время с последующим кодированием в бинарную последовательность (1). В качестве зависимой аппаратной составляющей используется системное смещение процессора с добавлением сокета процессора по следующему листингу:

id = “$(cat /proc/cpuinfo | grep 'model name' | uniq)”
auth = ”date +%s”
stamp = “$(echo -n “$id$auth” | xxd)”

$$TOTP = \left[\frac{T_1 - T_0}{T}\right] \cdot X, \quad (1)$$

где *TOTP* – временной код авторизации на сервере;

T_1 – текущее время, синхронизированное с онлайн-сервисами;

T_0 – начало времени по UTC (команда – *date +%s*);

X – время действия текущего отпечатка.

После того как устройства были первоначально идентифицированы, происходит проверка параметров их соединения по защищенному протоколу. Данный процесс проиллюстрирован на рисунке 2.

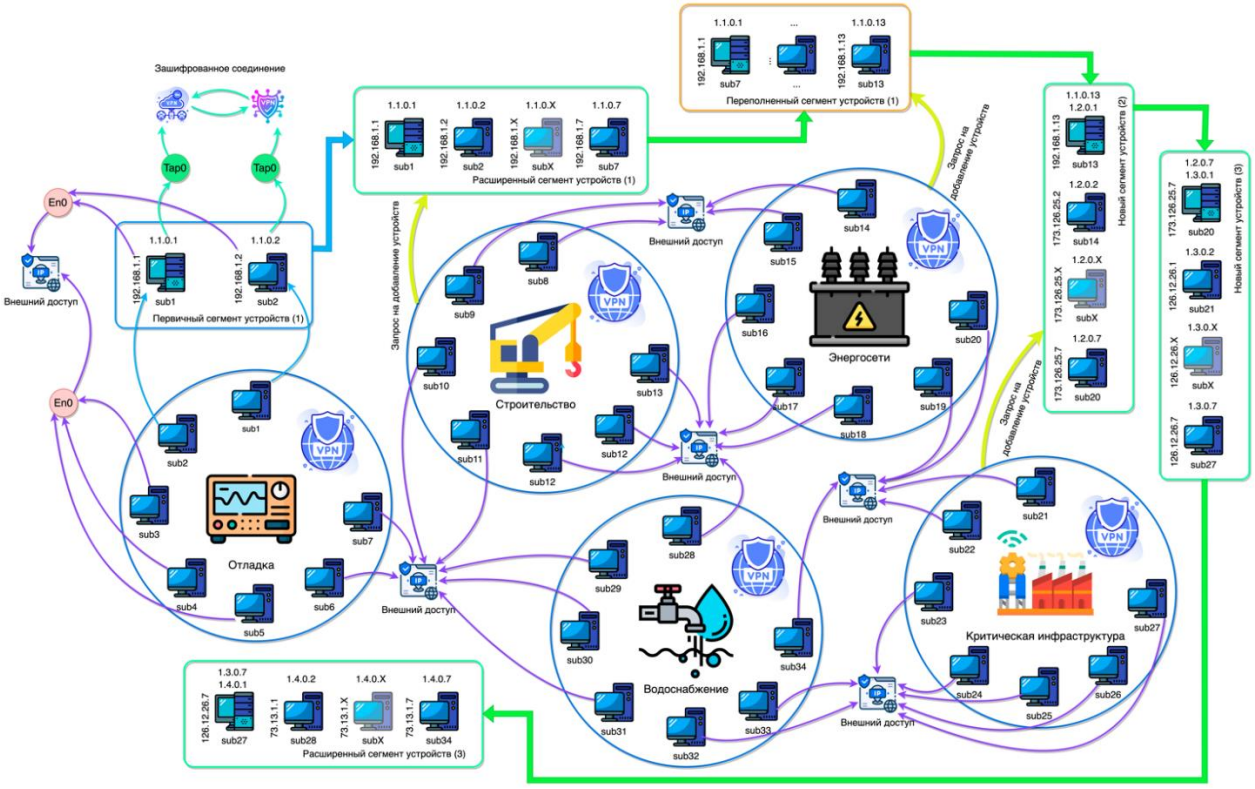

Рис. 2. *Типовая структура маршрутизации сегментов теплотехнологических сетей*

Fig. 2. *Typical structure of routing segments of thermal technology networks*

Согласно представленной топологии устройства, находящиеся в выделенных сегментах, обладают характеристиками, такими как *MAC*-адрес, *IP*-адрес, смещение *SoC*, а также максимальная и минимальная частота процессора (ГГц). Перечисленные характеристики, за исключением динамической частоты процессора, являются статичными и могут быть использованы для конфигурации ключей клиента/сервера *VPN*-соединения на последующих этапах. Для инициализации туннеля в рамках *OpenVPN (OVPN)* используются определенные параметры, перечисленные ниже:

- пул выделяемых адресов для меша – данный параметр определяет наличие массива или стартового *IPv4*-адреса для назначения клиентам сегмента сети;
- ограничения для резервирования – данный параметр предоставляет возможность задать ограниченное количество подключаемых устройств;
- открытый/закрытый ключ сервера – уникальная последовательность, генерируемая в форме *RSA*-ключа, используется для авторизации клиентов;
- авторизация по паролю – этот параметр является опциональным и позволяет использовать единый сертификат клиентов для авторизации по связке логин/пароль.

Для реализации *VPN*-топологии предполагается использовать параметры с динамическим счетчиком для пула адресов, начиная со второй ячейки, и стандартным значением в 10 устройств для ограничения резервирования [11, 12]. В качестве открытого/закрытого ключа сервера предлагается использовать 2054-битное *RSA*-шифрование с авторизацией по связке логин/пароль.

Таким образом, в качестве клиентов динамической системы предполагается использование единого сертификата с динамической системой генерации паролей по *TOTP*-смещению времени.

Для решения проблемы неравномерного распределения трафика предлагается применение собственного модуля распределения нагрузок со стороны клиентских устройств. Этот подход обеспечит возможность контроля трафика внутри сегмента сети со стороны клиента путем принудительного перенаправления запросов клиентов в локальный сетевой интерфейс. В результате этап прогнозирования нагрузок в теплотехнологических системах может быть реализован как отдельный модуль анализа трафика для устройств, которые выступают в роли серверов для *n*-го меша (рис. 3). Данный модуль может быть представлен в виде набора субпроцессов, включающих в себя компоненты, представленные ниже.

- Процесс «Первичное получение устройств сети» осуществляет запрос к серверу *OpenVPN (OVPN)* для получения списка доступных устройств по внутреннему *IP*-адресу, представленному в виде интерфейса *tap0*. Данный процесс является необходимым для определения активных устройств в сегменте.

- Процесс «Сегментация устройств» осуществляет разбивку выделенного пула устройств на несколько подсетей, содержащих от 2 до 10 устройств. Это позволяет точечно перенаправлять трафик в локальный интерфейс *lo* для контроля трафика со стороны клиента.

- Процесс «*Speedtest API*» предназначен для выполнения базовых замеров скорости загрузки и отдачи трафика с внешних серверов, чтобы определить текущую нагрузку сети.

- Процесс «Тестовое отключение устройств» направлен на отключение выбранного массива устройств с последующим выполнением «*Speedtest API*» для замеров нагрузки сети. Данный процесс позволяет провести анализ нагрузки сети при уменьшении количества активных устройств.

- Процесс «Принятия решений» использует результаты нескольких выходных данных *Speedtest API* для аналитического сравнения изменений при тестовых отключениях устройств. Этот подпроцесс позволяет принимать решение о продолжении работы или деаутентификации выбранного устройства в сегменте сети на основании анализа текущей нагрузки сети.

Из рисунка 3 следует, что процесс прогнозирования изменений трафика включает предварительное разбиение устройств на сегменты, содержащие по 2 *IP*-адреса. Это позволяет осуществлять замер текущей скорости загрузки/отдачи трафика с последующим временным перенаправлением каждого из устройств в локальный интерфейс и повторными замерами. После этого записи сохраняются в базе данных. Далее для прогнозирования потребления трафика предлагается использовать обученную *LSTM-XGBoost* модель [13, 14]. Для улучшения точности прогнозирования трафика необходимо использовать комбинированную модель с градиентным бустингом. Эта модель принимает на вход данные о текущем и предыдущих потреблениях трафика для данного пользователя в виде векторов g_i и x_i соответственно, которые вместе представляют входную матрицу X_i [15]. Для инициализации *LSTM*-слоя используется функция активации *PReLU*, после чего выполняется прогнозирование значений в соответствии с формулой 2 [16, 17]. Применение комбинированной модели позволяет учесть внешние факторы, оказывающие влияние на потребление трафика, и повысить точность прогнозирования:

$$\tilde{y}_{t+i} = PReLU(\omega_i \cdot h_i + b_h), \quad (2)$$

где $\tilde{y}_{t+i}$ – функция возврата прогнозных значений; *PReLU* – функция активации Parametric rectified linear unit.

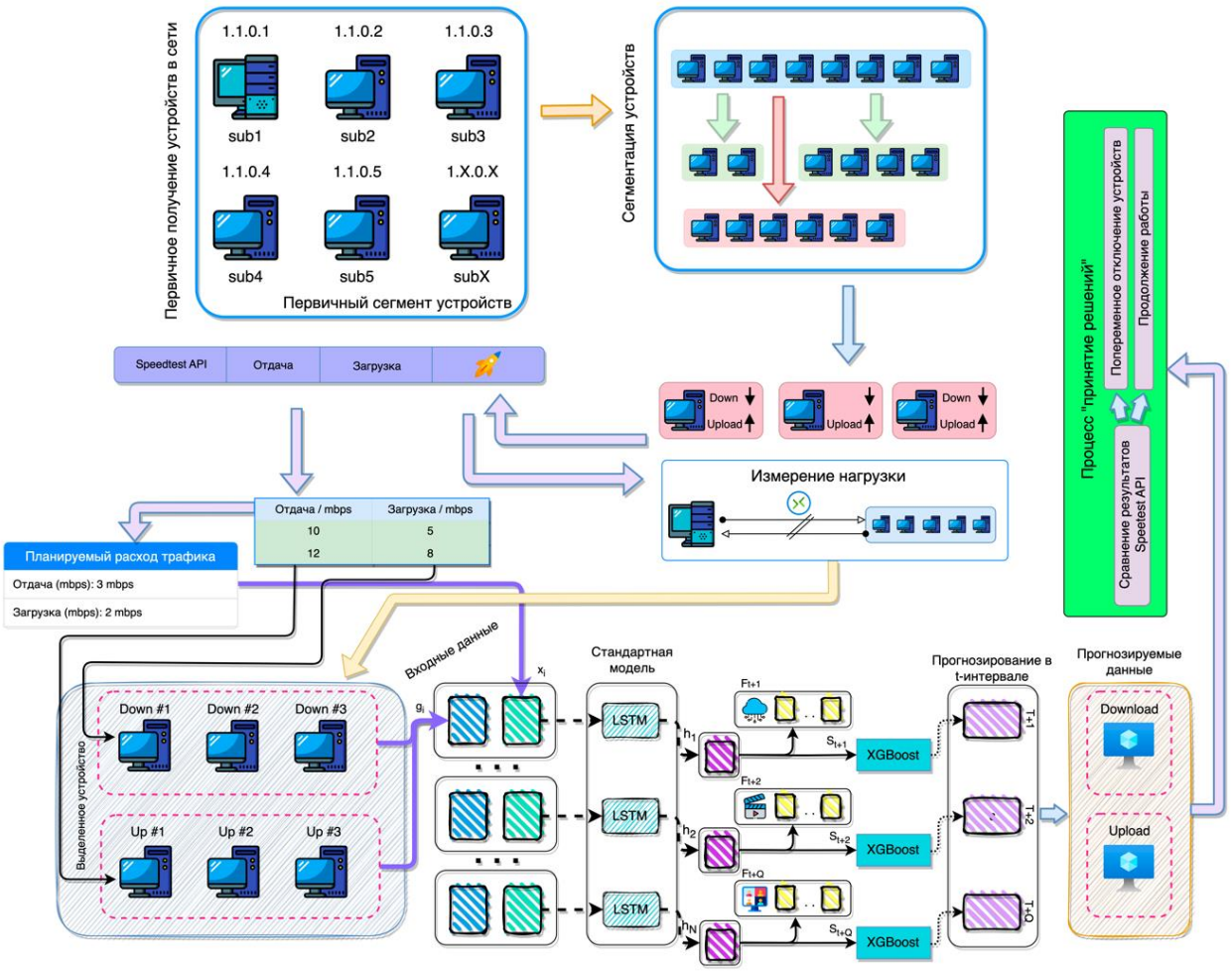

Рис. 3. *Организация процесса прогнозирования трафика при сегментации устройств*

Fig. 3. *Organization of the process of traffic forecasting during device segmentation*

На этапе выхода первичных векторов S_{t+Q} из *LSTM*-модели выполняется прогнозирование значений за счет *XGBoost*-модели в идентичном временном промежутке $\tilde{y}_{t+i}$ с учетом внешних факторов влияния на трафик, обозначенных F_{t+Q} в формуле

$$\hat{y}_{t+i} = \sum_{n=1}^{n} f_n(S_{t+Q}), \quad (3)$$

где $\tilde{y}_{t+i}$ – функция возврата прогнозных значений *XGBoost*; S_{t+Q} – выходные значения векторов из нейронной сети.

Таким образом, на данном этапе процесса прогнозирования трафика осуществляется получение выходных значений из *LSTM*-модели, после чего прогнозы уточняются при помощи градиентного бустинга. Такой подход позволяет получать более точные прогнозы возможной нагрузки на сеть с конкретного устройства, что обеспечивает возможность принятия оптимальных решений по оптимизации работы сегмента сети [18, 19].

Для реализации функции управления и принятия решений по обеспечению оптимальной нагрузки и безопасности предлагается использовать процесс первоначального нечеткого сравнения аутентифицируемой последовательности. Однако выходные данные формулы 1 и «склейки» *ID*-процессора на выходе представляют собой бинарную последовательность вида «00100101010…010101000». По умолчанию *TOTP*-генерация

значения времени обновляет выходную переменную каждую секунду, что может приводить к расхождениям в последовательностях при сравнении значений. Учитывая вышеизложенное, в данной системе применяется модуль нечеткого сравнения на базе библиотеки *FuzzyWuzzy*. Реализация модуля принятия решений основана на Python-модуле, который использует структуру данных *pandas* для первоначального сохранения результатов в файл «**.csv*» для последующей загрузки и сравнения через указанную библиотеку, как представлено на рисунке 4 [20].

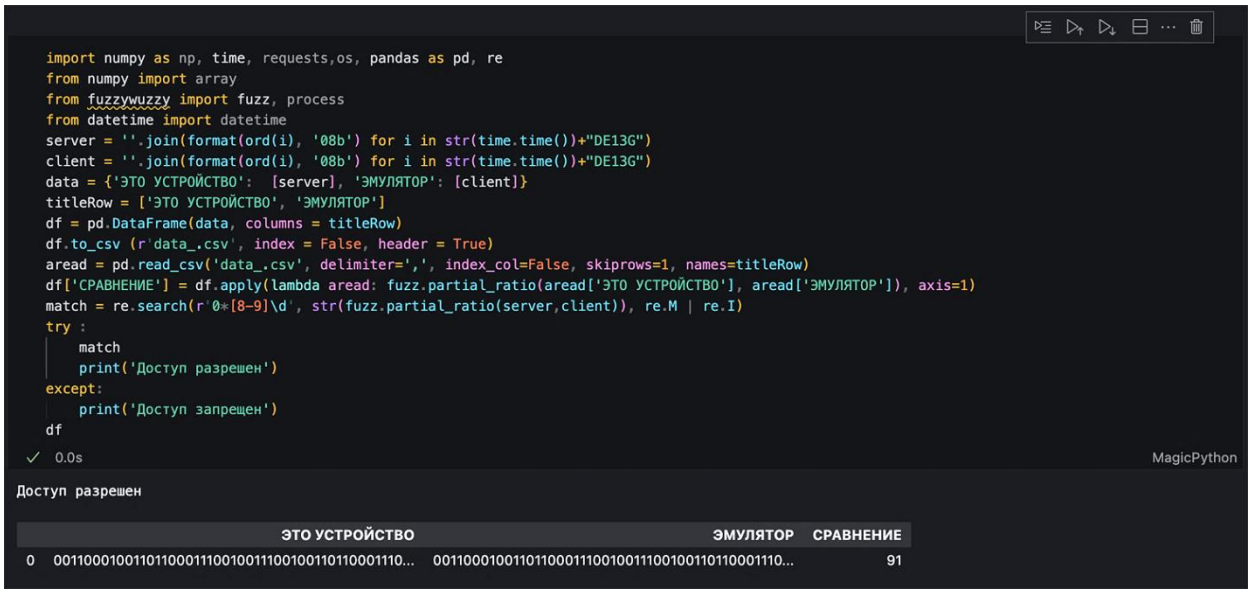

Рис. 4. *Тестирование модуля нечеткого посимвольного сравнения*

Fig. 4. *Testing the fuzzy symbol-by- symbol comparison module*

Процесс сравнения первичного кода включает в себя генерацию уникального временного отпечатка и уникального идентификатора агента. Этот набор данных затем преобразуется в двоичный код и сравнивается с помощью функции *partial math rate*, интегрированной в библиотеке *FuzzyWuzzy*. Результаты сравнения представлены в виде процента совпадения, который может варьироваться в зависимости от параметров настроек. Для установления валидности инициализируемого соединения используется регулярное выражение, которое гарантирует достижение процента совпадения на уровне 80 % и выше. В итоге использование модуля нечеткого сравнения на основе библиотеки *FuzzyWuzzy* позволяет установить достоверность и подлинность аутентифицируемых последовательностей в системе.

Заключение

В данной статье были проанализированы наиболее популярные из существующих решений построения модульных сетевых протоколов для организации функционирования сложных систем. Выявлена актуальная проблема распределения трафика и обеспечения безопасности при взаимодействии в сложных теплотехнологических системах. Предложена модель-топология клиент-серверного взаимодействия таких комплексов, а также отдельная система прогнозирования для принятия решений о доступе клиентов к сегментам сети с помощью реализованного алгоритма верификации доступа. Данное решение было реализовано в виде готового программного продукта. Важной чертой предлагаемого решения является децентрализованный подход взаимообмена на основе *mesh*-топологии, что может быть использовано для реализации полноценных автомати-

зированных платформ управления данными в корпоративных организациях. Реализованная топология благодаря своей многомодульности позволяет первоначально осуществлять соединение между субъектами сети и поддерживать обмен информацией с расширением устройств в сети за счет развертки на клиенте серверной составляющей *VPN*-сервера. Описана возможность отслеживания перегрузок трафика за счет совместного использования *LSTM*-сети с градиентным бустингом и системы прогнозирования. Особое внимание следует уделить реализованному модулю контроля трафика внутри сети. Модуль циклически запрашивает изменения скорости интернет-соединения с внешним сервером и прогнозирует превышения доступного лимита для оптимизации работы теплотехнологической сети. Также важной функциональностью является *ARP*-обработка трафика, которая помогает управлять потоками данных в сети. В целом разработанный программный модуль представляет собой инновационный подход к управлению теплотехнологическими комплексами, который может быть использован в широком спектре корпоративных организаций.

REFERENCES

1. Kensworth S., Saumitra A., Vahid D. et al. On the Design and Implementation of IP-over-P2P Overlay Virtual Private Networks. *IEICE Transactions on Communications.* 2020. Vol. E103.B. No. 1. P. 2–10. DOI: https://doi.org/10.1587/transcom.2019CPI0001

2. Zhang Y., Zhong N., You W. et al. NDFuzz: a non-intrusive coverage-guided fuzzing framework for virtualized network devices. *Cybersecurity.* 2022. No. 5(21). DOI: https://doi.org/10.1186/s42400-022-00120-1

3. Seneviratne P. Beginning LoRa Radio Networks with Arduino: Build Long Range, Low Power Wireless IoT Networks. New York: Apress, 2019. 320 p.

4. Ahmadi A.E. An Introduction to Wireless Mesh Networks. New York: Scholars' Press. 2022. 68 p.

5. Kim J.-W., Kim J., Lee J. Cross-Layer MAC/Routing Protocol for Reliability Improvement of the Internet of Things. *Sensors.* 2022. Vol. 22(9429). DOI: https://doi.org/10.3390/s22239429

6. *Моисеев В. И.* Экспериментальное исследование структуры пакетного буфера Ethernet коммутатора. *T-Comm.* 2020. № 1. С. 18–24.

Moiseev V.I. *Eksperimental'noe issledovanie struktury paketnogo bufera Ethernet kommutatora* **[**Experimental evaluation of ethernet switch packet buffer structures]. *T-Comm*. 2020. No. 1. Pp. 18–24. (In Russian)

7. *Канаев А. К., Логин Э. В., Гришанов И. С.* Комплексный алгоритм процессов контроля и управления телекоммуникационной сетью Carrier Ethernet с применением механизмов OAM // Известия Петербургского университета путей сообщения. 2022. Т. 19. Вып. 2. С. 266–275. DOI: 10.20295/1815-588X-2022-2-266-275

Kanaev A.K., Login E.V., Grishanov I.S. Complex Algorithm for Control and Management Processes of Carrier Ethernet Telecommunication Network Using OAM Mechanisms. *Proceedings of Petersburg Transport University*. 2022. Vol. 19. No. 2. Pp. 266–275. DOI: 10.20295/1815-588X-2022- 2-266-275. (In Russian)

8. *Никишин К. И.* Исследование передачи трафика в программно-конфигурируемой сети с использованием cisco packet tracer // ВГТУ. 2022. № 5. С. 85–90.

Nikishin K.I. Modeling a wireless sensor network using OMNET. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Bulletin of Ryazan State Radio Engineering University]. 2022. No. 5. Pp. 85–90. (In Russian)

9. Simla J.A., Chakravarthy R., Leo M.L. An Experimental study of IoT-Based Topologies on MQTT protocol for Agriculture Intrusion Detection. Measurement: Sensors. 2022. Vol. 24. DOI: https://doi.org/10.1016/j.measen.2022.100470

10. Wang M., Li Y., Lv J., Gao Y., Qiao C., Liu B., Dong W. ACE: A Routing Algorithm Based on Autonomous Channel Scheduling for Bluetooth Mesh Network. *Electronics*. 2022. No. 11(113). DOI: https://doi.org/10.3390/electronics11010113

11. *Андреев С. В., Хлупина А. А.* Оптимизация скорости vpn для удаленной работы с использованием маршрутизаторов с arm-процессорами // Программные продукты и системы. 2020. № 4. С. 605–612.

Andreev S.V., Khlupina A.A. Optimizing speed for VPN providing the possibility of telework using routers powered by ARM CPU. Programmnye produkty i sistemy. *Software & Systems*. 2020. No. 4. Pp. 605–612. (In Russian)

12. *Мартьянов А. В.* Анализ информации о подключениях к сети предприятия удаленных пользователей // Инновационная наука. 2021. № 6. С. 46–48.

Martyanov A.V. Analysis of information about connections to the enterprise network of remote users. *Innovacionnaya nauka* [Innovative science]. 2021. No. 6. Pp. 46–48. (In Russian)

13. Zaenchkovsky A., Kirillova E., Zeman Z. Mathematical foundations intellectually coordination of data for group expert innovative processes evaluation within the framework of scientific and industrial cooperation. Algorithms and solutions based on computer technology. *Lecture Notes in Networks and Systems.* Vol. 387. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-93872-7_9

14. Dai Y., Zhou Q., Leng M. et al. Improving the bi-LSTM model with XGBoost and attention mechanism: A combined approach for short-term power load prediction. Applied Soft Computing. 2022. No. 130. DOI: https://doi.org/10.1016/j.asoc.2022.109632

15. *Борисов В. В., Булыгина О. В., Дли М. И., Козлов П. Ю.* Рубрицирование текстовых документов на основе нечетких отношений различия // Прикладная информатика. 2020. Т. 15. № 3. С. 36–45. DOI: 10.37791/2687-0649-2020-15-3-36-45

Borisov V.V., Bulygina O.V., Dli M.I., Kozlov P.Yu. Rubrication of text documents based on fuzzy difference relations. *Prikladnaya informatika* [Journal of Applied Informatics]. 2020. Vol. 15. No. 3. Pp. 36–45. DOI: 10.37791/2687-0649-2020-15-3-36-45. (In Russian)

16. Pajankar A., Joshi A. Hands-on Machine Learning with Python: Implement Neural Network Solutions with Scikit-learn and PyTorch. New York: Apress, 2022. 356 p.

17. *Чумакова Е. В., Корнеев Д. Г., Гаспариан М. С.* Подход к проектированию нейронной сети для формирования индивидуальной траектории тестирования знаний // Прикладная информатика. 2022. Т. 17. № 5. С. 102–115. DOI: 10.37791/2687-0649-2022-17-5-102-115

Chumakova E.V., Korneev D.G., Gasparian M.S. An approach to the design of a neural network for the formation of an individual trajectory of knowledge testing. *Prikladnaya informatika* [Journal of Applied Informatics]. 2022. Vol. 17. No. 5. Pp. 102–115. DOI: 10.37791/2687-0649-2022-17-5-102-115. (In Russian)

18. *Непомнящий О. В.* Метод оценки ресурсов в процессе функционально-потокового высокоуровневого синтеза СБИС // Прикладная информатика. 2022. Т. 17. № 3. С. 34–44. DOI: 10.37791/2687- 0649-2022-17-3-34-44

Nepomnyashchiy O.V. Resource estimation method in the process of functional-flow high-level VLSI synthesis. *Prikladnaya informatika* [Journal of Applied Informatics]. 2022. Vol. 17. No. 3. Pp. 34–44. DOI: 10.37791/2687-0649-2022-17-3-34-44. (in Russian)

19. Park M.-H., Chakraborty S., Vuong Q.D. et al. Anomaly detection Babed on time series data of hydraulic accumulator. *Sensors.* 2022. Vol. 22(9428). DOI: https://doi.org/10.3390/s22239428

20. Chen G., Tat T.P. Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems. 1st ed. Boca Raton: CRC Press, 2019. 328 p.

Информация об авторах

Окунев Борис Васильевич, канд. техн. наук, доцент, преподаватель кафедры информационных технологий в экономике и управлении, Национальный исследовательский университет «Московский энергетический институт» – филиал в г. Смоленске;

214013, Россия, г. Смоленск, Энергетический проезд, 1;

ok-bmw@rambler.ru, ORCID: https://orcid.org/0000-0001-8740-7855

Верейкина Елизавета Константиновна, аспирант, Национальный исследовательский университет «Московский энергетический институт»;

111250, Россия, Москва, Красноказарменная улица, 17;

vereikina.ek@mail.ru, ORCID: https://orcid.org/0000-0003-3791-9099

Лазарев Алексей Игоревич, ассистент кафедры информационных технологий в экономике и управлении, Национальный исследовательский университет «Московский энергетический институт» – филиал в г. Смоленске;

214013, Россия, г. Смоленск, Энергетический проезд, 1;

anonymous.prodject@gmail.com, ORCID: https://orcid.org/0000-0003-3252-0409

Information about the authors

Okunev Boris Vasilievich, Candidate of Technical Sciences, Associate Professor, Teacher of the Department of Information Technologies in Economics and Management, National Research University “Moscow Energy Institute” – branch in Smolensk;

214013, Russia, Smolensk, 1 Energetichesky proezd;

ok-bmw@rambler.ru, ORCID: https://orcid.org/0000-0001-8740-7855

Vereykina Elizaveta Konstantinovna, Graduate student of the National Research University “Moscow Energy Institute”;

111250, Russia, Moscow, 17 Krasnokazarmennaya street;

vereikina.ek@mail.ru, ORCID: https://orcid.org/0000-0003-3791-9099

Lazarev Alexey Igorevich, Assistant of the Department of Information Technologies in Economics and management, National Research University “Moscow Energy Institute” – branch in Smolensk;

214013, Russia, Smolensk, 1 Energetichesky proezd;

anonymous.prodject@gmail.com, ORCID: https://orcid.org/0000-0003-3252-0409