УДК 004.056.5, 004.8 doi: 10.15827/0236-235X.142.442-450 2023. Т. 36. № 3. С. 442–450

Организация адаптивной маршрутизации данных в электроэнергетических комплексах с использованием онтологических нечетких классификаторов

А.С. Федулов
А.И. Лазарев

Ссылка для цитирования
Федулов А.С., Лазарев А.И. Организация адаптивной маршрутизации данных в электроэнергетических комплексах с использованием онтологических нечетких классификаторов // Программные продукты и системы. 2023. Т. 36. № 3. С. 442–450. doi: 10.15827/0236-235X.142.442-450
Информация о статье
Поступила в редакцию: 29.05.2023 После доработки: 04.07.2023 Принята к публикации: 05.07.2023

Аннотация. В работе рассматриваются теоретические аспекты применения методов машинного обучения, в частности, адаптация глубоких моделей к управлению сетевыми топологиями TCP/IP электроэнергетических комплексов. Предметом исследования является подход к организации централизованного управления сегментами сети в рассматриваемой сфере. Изучение процессов взаимодействия субъектов электроэнергетических подразделений на основе разработанных онтологических моделей позволило выявить основные свойства полиформатных данных, которые могут быть уязвимыми при эксплуатации. Практическая значимость исследования заключается в создании многомодульной структуры отслеживания, классификации и прогнозировании изменений в потребляемом трафике, за счет которой возможно повышение эффективности функционирования сложных сетевых корпоративных структур. Проведено тестирование существующих алгоритмов получения хеш-функций. Его результаты позволили сделать вывод о целесообразности применения базового алгоритма шифрования BLAKE3 в качестве основного механизма верификации подлинности клиентов в сравнении с алгоритмами SHA-384, SHA-512, SHA-224, MD5. Показана реализация алгоритма нечеткого посимвольного сравнения в качестве модуля принятия решений, что подтверждает актуальность предлагаемого подхода при работе с нечеткими структурами данных. В качестве основного решения указанных проблем предложен подход к гибкому управлению сегментом электроэнергетических установок, представляемых комплексом генерирующих, электросетевых, энергосбытовых и других компаний. Основным результатом предлагаемого решения является централизованный анализ возможных изменений с учетом адаптации к сетевым нагрузкам на основе выделенных онтологических переменных. При реализации данного подхода возможна совместимость с существующими аппаратными сетевыми устройствами за счет уникальной архитектуры построенной топологии.

Ключевые слова: электроэнергетические комплексы, онтологические модели, классификация данных, принятие решений, нечеткая логика, обеспечение безопасности, глубокое обучение
Благодарности. Работа выполнена в рамках государственного задания, проект № FSWF-2023-0012

Совокупность множества управляемых электросетевых, энергосбытовых компаний, включая энергосистемы и подразделения поддержки коммерческой инфраструктуры российского рынка, представляет собой электроэнергетический комплекс, осуществляющий бесперебойное снабжение потребителей необходимыми средствами [1, 2]. Развитие данной области сопровождается активным внедрением IT-технологий в процессы автоматизации деятельности, отслеживания неполадок и проведения критически важных испытаний. Идентичные структуры и процессы присущи также электромеханическим и теплотехнологическим системам.

Развитие подразделений в указанных инфраструктурах поддерживается внедрением сетевых структур на базе протоколов TCP/IP, включая функциональные возможности резервирования важных данных, поддержки отказоустойчивости, оперативного изменения состава сегментов предприятия. Существенная часть как аппаратных (cisco, microtik), так и программных (pfSense, NethServer, ClearOS) решений поддерживают интеллектуальное управление трафиком клиентов с учетом корректной настройки маршрутизации до конечного клиента [3, 4]. Вместе с тем существует ряд проблем, основной из которых является правильность настройки сетевого оборудования, включая возможное взаимодействие IoT-оборудования (Internet of Things) с аппаратными техническими комплексами (рис. 1). Исследования в области оптимизации адресации TCP/IP проводятся многими учеными. Так, в статье [5] авторы предлагают решить проблему недостаточности выделяемого пула в маршрутизаторах малого офиса за счет изменения операционной системы OpenWRT. Данный подход позволяет частично решить указанную проблему оптимизированной доставки трафика клиентам, однако остается актуальной проблема адаптации к другим операционным системам при использовании альтернативных

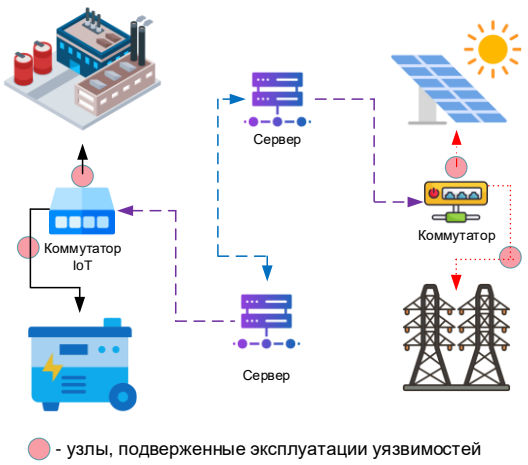

Рис. 1. Топология взаимодействия устройств электроэнергетических структур

Fig. 1. A topology of electric power structures device interaction

поставщиков сетевого оборудования. В публикации [6] описан процесс разработки протокола туннелирования с использованием IPv6-адресации и перезаписи полей заголовков для идентификации клиента, представлены перспективные направления в развитии методов безопасной передачи данных. Предлагаемое решение обладает новизной в области прогнозирования изменений в сетевом трафике. В то же время возможности использования обученных моделей не предполагают дополнительных затрат на усовершенствование аппаратной составляющей электроэнергетических комплексов.

Представленная на рисунке 1 топология взаимодействия затрагивает два магистральных узла, а также ряд устройств, напрямую взаимодействующих с управляющими электроэнергетическими установками. Нарушение корректной конфигурации в одном из узлов топологии (выделены круговыми указателями) может повлечь за собой ряд проблем. Среди них можно выделить перегрузку трафика на каком-либо узле сети, а также нарушение конфиденциальности из-за использования устаревших версий протоколов и ПО (включая полнофункциональный доступ к узлу сети), что подтверждает актуальность исследования.

Для решения указанных проблем предлагается система управления сетевыми топологиями TCP/IP в электроэнергетических комплексах с использованием данных онтологической модели для автоматизации процессов принятия решений по оптимизации работы сегментов сети.

Исследование основных параметров эксплуатации уязвимостей на базе онтологических моделей

Рассматривая большую часть уязвимостей и полезных нагрузок на ресурсах OffSec (https://www.exploit-db.com), предполагающих прямое или косвенное воздействие на программную платформу информационных структур, следует обратить внимание на таргетированные атаки на протоколы доставки данных. Различия в данной базе определяются конкретным портом приложения: на текущий момент насчитывается более 300 портов приложений и служб, для которых существуют уязвимости различных уровней.

Для решения потенциальных проблем с обеспечением безопасности компаний, являющихся поставщиками сервисов, на постоянной основе предлагают клиентам возможность своевременного обновления интегрируемого ПО. Вместе с тем часть специфических программных средств могут напрямую зависеть от аппаратной составляющей, изменение которой в большинстве случаев нерентабельно. Альтернативной проблемой является некорректность конфигурации одного или нескольких узлов сетевых топологий, приводящая к нарушению конфиденциальности – зачастую организации на территории РФ используют технологии на стадии альфа-релиза.

В качестве основного подхода к реализации оптимального управления электроэнергетическими структурами предлагается онтологическая модель, изображенная на рисунке 2. Она представляет собой совокупный набор большинства полиформатных данных, обрабатываемых на электроэнергетических комплексах. Как можно увидеть из этой модели, на текущий момент основными сервисами для обработки данных являются приложения, работающие на портах 20, 21, 25, 80, 443, 3306, 3389, 110 [7, 8]. Указанные порты в большинстве случаев являются стандартными для доступа к интерфейсу управления, что также нарушает политику информационной безопасности.

Условное подразделение, представленное на рисунке 2, указывает на множественные точки уязвимостей, например, внедрение вредоносного исполняемого кода в передаваемый файл, изменение и перехват аудио- и видеопотока, использование слабых ключей шифрования к удаленному терминалу, а также обеспечение удаленного управления через устаревшие версии протоколов RDP/VNC.

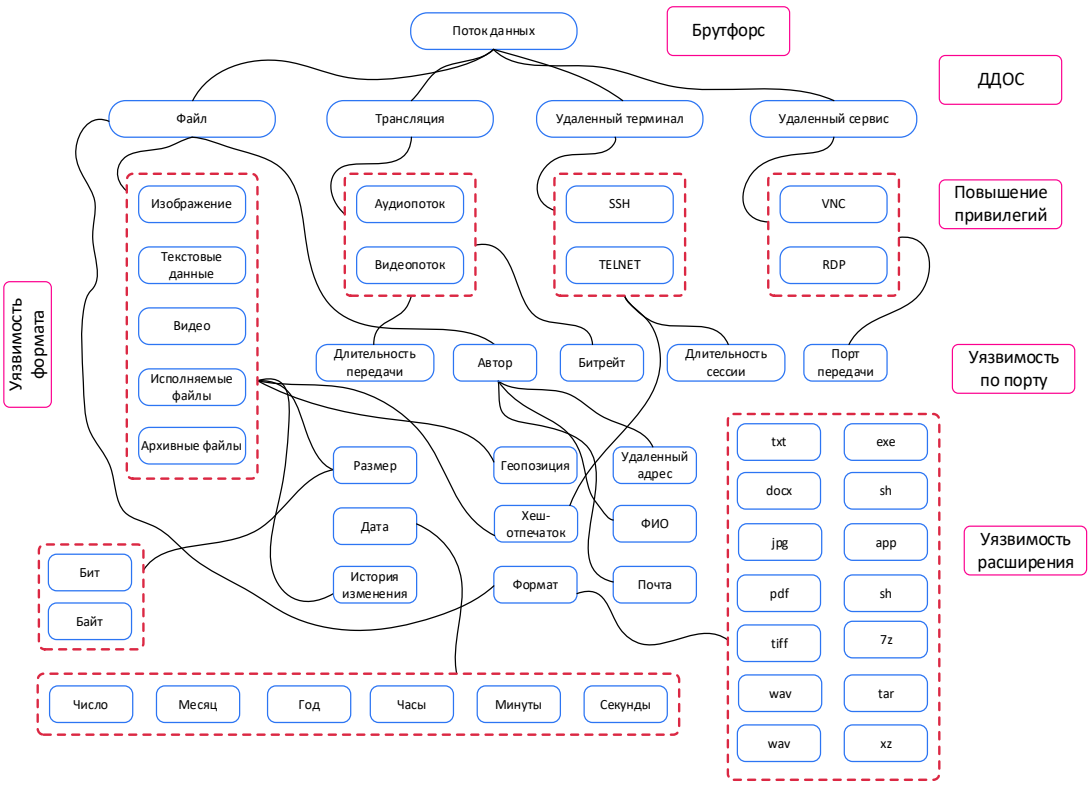

Рис. 2. Онтологическая модель передачи данных в электроэнергетическом комплексе

Fig. 2. An ontological model of data transmission in an electric power complex

Использование данной онтологической модели в процессе разработки программного алгоритма также позволяет выявить основные изменяемые третьими лицами показатели для маскировки изменений в оригинальной сигнатуре, такие как хеш файла, информация об авторе, геолокация. В качестве основных примеров реализации уязвимостей можно привести CVE-2019-0708, CVE-2019-1935, CVE-2020-0688, некоторые из них не требуют дополнительного вмешательства со стороны атакуемого лица.

Рассматривая структуру обмена данными между пользователями, можно выделить основные отличия передаваемых данных (рис. 3). Выделяемые классификации трафика позволяют в последующем оптимизировать работу отдельных подсетей для обеспечения минимальной задержки взаимодействия с внешним сервером.

Результат рассмотрения представленных моделей, в частности, упрощенной модели классификации трафика, позволяет в последующей реализации подхода оптимизации сети электроэнергетических образований выделить основные факторы (параметры), используемые в дальнейшем как главные прогнозируемые показатели в системе принятия решений по управлению сегментированными участками.

Разработка многомодульной системы управления электроэнергетическими структурами

Немаловажной составляющей при разработке интеллектуального подхода к управлению сетевыми структурами электроэнергетических комплексов являются алгоритмы определения ключевых устройств в сегменте сети, а также выявления возможных мест эксплуатации уязвимостей в соответствии с представленной онтологической моделью классификации данных. В предлагаемом алгоритме интеллектуального управления (рис. 4) основным является первичный анализ доступных устройств в сегменте сети с последующим выявлением доступных портов (глубокое сканирование) для классификации трафика и обучения глубокой модели.

Как видно из представленного алгоритма, процесс оптимизации нацелен на внесение

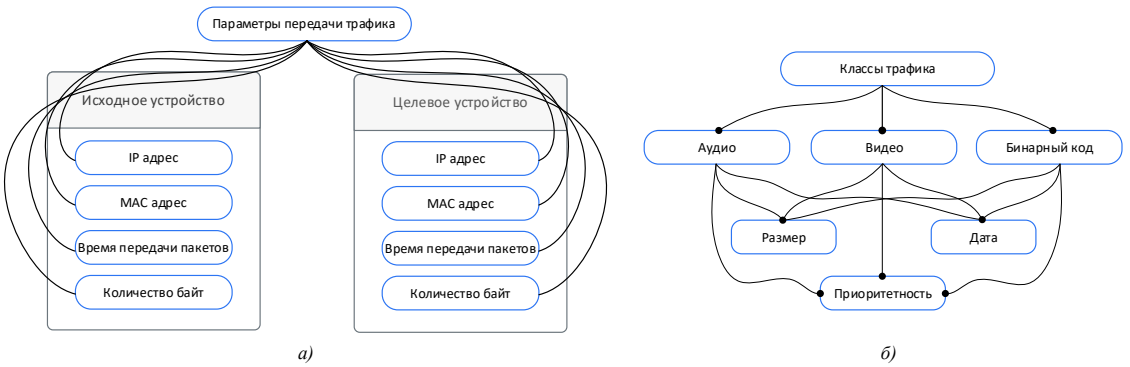

Рис. 3. Обмен данными между пользователями: а) онтологические модели набора параметров в пакетах трафика; б) упрощенная модель разделения трафика

Fig. 3. Data exchange between users: a) parameter set ontological models in traffic packets; b) a simplified traffic separation model

изменений в реальном времени с учетом выявленных отклонений в соответствии с первоначальной сетевой топологией TCP/IP. Этапы сопоставления предиктивного трафика с реальными данными, изменения маршрутизации на основе расходуемого трафика, принятия решений по изменению топологии в данном алгоритме обособлены из-за изменчивости структуры электроэнергетических систем, то есть добавления или удаления различных сегментов.

С учетом выделенной топологии взаимодействия устройств и алгоритма интеллектуального управления электроэнергетическими структурами была разработана углубленная топология взаимодействия устройств (http://www.swsys.ru/uploaded/image/2023-3/2023-3-dop/15.jpg).

В качестве основной программной составляющей предполагается наличие базового DHCP сервера разделения сегментации (dhcpd), виртуальных компьютерных сетей (VLAN), а также нескольких управляемых точек виртуальных внешних сетей (VPN), инициализируемых сервером WireGuard/OVPN [9]. Выделяя возможные подразделения сегментов сети, следует отметить, что соединение выделяемых подразделений осуществляется через виртуальный сегмент с использованием частных виртуальных сетей.

Организация процесса классификации трафика в данном решении основана на применении дополнительных средств анализа выходных данных фреймворка NFStream [10]. Используемый пакет задействует глубокий анализ пакетов за счет выделения множества параметров начальной и конечной точек IP-адресации, задержки отправки и получения данных, количества выходной и входной информации (в байтах), а также размера пакетов и нагрузки сети. В качестве основного средства для прогнозирования изменений в трафике используется библиотека numpy с последующей записью данных в датафрейм (библиотека pandas).

Процесс прогнозирования и сравнения изменений в трафике выглядит следующим образом:

```
   # import lib
   import numpy
   import datetime
   import pandas as pd

   class ModelPrediction(NFPlugin):
      # Flow initialization method
      def on_initial(self, packet, flow):
         flow.udps.model_prediction = 0
      # Method called when updating the
stream
      def on_update(self, flow):
         to_predict = numpy.array([flow.
bidirectional_packets,
               flow.bidirec-
tional_bytes]).reshape((1,-1))
      flow.udps.model_prediction = self.
my_model.predict(to_predict)

   ml_streamer = NFStreamer(source="en0",
udps=ModelPrediction(my_model=model))
   # Writing data to pandas
   data = ml_streamer.to_csv(path=None,
columns_to_anonymize=[],
flows_per_file=0, rotate_files=0
```

Очевидно, что в модели прогнозирования используется процесс захвата потока из адаптера en0 с последующим сохранением в csv-файл – в качестве основных параметров для прогнозирования используются bidirectional packets, bidirectional_bytes, составляющие ак-

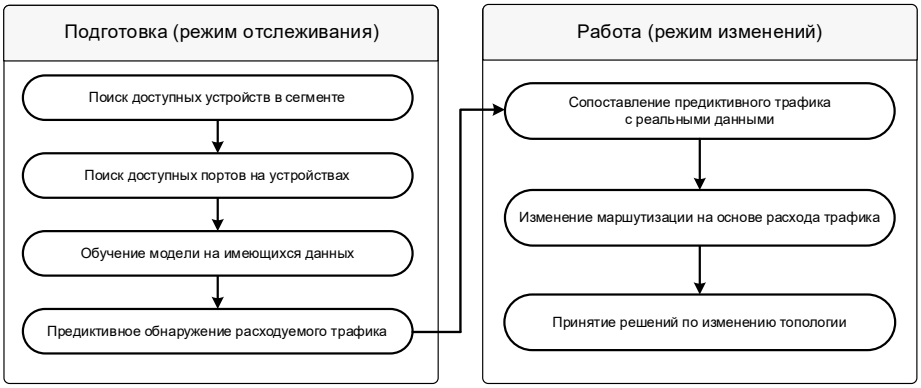

Рис. 4. Алгоритм адаптации топологии электроэнергетических комплексов

Fig. 4. An algorithm for adapting the topology of electric power complexes

кумулятор потоков и количество байтов для двунаправленных пакетов.

В качестве дополнительных средств для прогнозирования изменений в возможных превышениях трафика предлагается использование глубокой модели на основе выходных данных pcap-файла как входных данных для обучения сети [11]. Основу предлагаемой нейронной сети составляет модель Long-Short Term Memory (LSTM), предоставляющая возможность долговременного хранения зависимостей [12].

Продемонстрируем работу слоя фильтра забывания:

$$g_t = \sigma(W_{xf} x_t + W_{xf} h_{t-1} + W_{cf} c_{t-1} + b_f),$$

входной слой:

$$l_t = g_t c_{t-1} + \sigma(W_{xi} x_t + W_{xi} h_{t-1} + W_{ci} c_{t-1} + b_i) \times$$
$$\times \tanh(W_{xc} x_t + W_{hc} h_{t-1} + b_c),$$

а также выходной:

$$h_t = \sigma(W_{xo} x_t + W_{ho} h_{t-1} + W_{co} c_t + b_o \tanh(c_t)),$$

где W, b – обучаемые параметры; σ, tanh – функции активации [13].

Программная реализация модели LSTM основана на библиотеке Keras. Модель включает слои *Dense*, *LSTM*, *SimpleRNN*, основное количество нейронов для которых – 1, 4, 3 соответственно [14]. Главной функцией оптимизатора является adaptive moment estimation (adam) с целевым параметром потерь – расчет среднеквадратичной ошибки:

$$R = \sqrt{\frac{\sum_{i=1}^{N} || y(i) - \hat{y}(i) ||^2}{N}},$$

где $y(i)$ – i-я итерация изменений; N – количество данных; $\hat{y}(i)$ – прогноз.

Таким образом, при использовании комбинации фреймворка NFStream и сторонней LSTM-модели возможно получение как данных по классификации трафика, так и прогнозируемых значений по расходуемому трафику в различных периодах.

Разработка модуля обеспечения безопасного функционирования электроэнергетической TCP/IP-топологии

Немаловажной составляющей в процессе TCP/IP-взаимодействия является шифрование данных с использованием как протоколов защиты трафика, например, SSL, VPN, так и средств шифрования данных на стороне клиента. Существующие средства туннелирования трафика в большинстве случаев основаны на первичной установке клиент-серверных корневых сертификатов, обмене двухсторонними ключами (подключение как пира), а также применении пары логин–пароль. Альтернативная поддержка обеспечения безопасности также возможна путем сертификации с использованием SSL-шифрования в случаях взаимодействия с веб-приложениями, однако актуальным остается вопрос обеспечения безопасности при проведении таргетированных атак на отдельные службы и сервисы. Как можно увидеть из представленной на рисунке 1 онтологии, непреднамеренное использование хотя бы одного из уязвимых сервисов может привести к утечке данных, следующей за несанкционированным доступом.

Для решения проблемы предлагается использование средств хеширования на основе алгоритма BLAKE3 с последующим комбинированием TOTP-алгоритма обновления ключей шифрования, реализующих совокупный

алгоритм беспрерывной аутентификации субъектов. Алгоритм шифрования BLAKE3 является хорошей альтернативой существующим хеш-функциям, предоставляя возможность быстрого получения зашифрованного сообщения наряду с надежностью, идентичной SHA-3. В качестве основного тестирования производительности была проведена проверка вычисления хеш-суммы двоичного файла размером 1 Гб на процессоре MAC M1 и построен график (http://www.swsys.ru/uploaded/image/2023-3/2023-3-dop/16.jpg).

Согласно результатам последовательного тестирования указанных функций можно заключить, что для расчета хеш-функции алгоритму SHA-224 требуется 3,708 сек., в то время как алгоритму BLAKE3 – 0,18 сек.

С учетом того, что при TOTP-шифровании важным является процесс обновления функции за определенный фиксированный интервал, наиболее целесообразно применение алгоритма шифрования BLAKE3. Его алгоритмическая составляющая образована за счет комбинирования средств предыдущего хеш-шифра (BLAKE2) и утилиты Bao, что в совокупности снимает ограниченное ветвление (рис. 5). На основании рисунка можно заключить, что архитектура ограничивается блоками по 1 024 байта, при которых возможно переполнение с последующим образованием двух родительских узлов, причем переполнение возможно начиная с предоставления 1 байта для следующего фрагмента.

Для организации процесса динамического обновления ключа предлагается использовать TOTP-генерацию зависимого ключа, образуемого по формуле

$$\text{BLAKE3(VALUE)} = \text{CLIENT}_{id},$$

$$\text{VALUE(ID)} = \left[\frac{T_1 - T_0}{T}\right] \cdot \text{DELAY},$$

где VALUE – цифровой временный отпечаток; BLAKE3 – общий идентификатор для пары устройств, образуемый от VALUE и хеш-функции; T_1 – текущее системное время; T_0 – статичный параметр времени; DELAY – время действия отпечатка; CLIENT_{id} – идентификатор пары.

Программная реализация указанного метода осуществляется с учетом передаваемого потока информации: предлагаемое решение за счет своей гибкости позволяет вычислять цифровые отпечатки для определенных данных, действительных в течение *n*-го времени.

Разработка модуля принятия решений по изменению структуры распределения трафика TCP/IP

Немаловажным компонентом в реализации указанного подхода является система принятия решений по изменению структуры в отдельных частях топологии сети TCP/IP. В большинстве случаев принятие автоматизированных решений нацелено на работу с достаточными данными либо с алгоритмами машинного обучения на нечеткой основе. С учетом ранее предложенных методов классификации трафика, прогнозирования скорости загрузки и отдачи через WAN-канал предлагается использовать автоматизированные функции вычисления возможных совпадений при линейном сравнении с оригинальными выходными данными.

Как сказано ранее, фреймворк NFStream обладает возможностью прогнозирования классов трафика, в то время как реализованный подход к прогнозированию потребления трафика на основе LSTM-моделей позволяет получать возможные значения по потреблению. Использование выходных данных указанных модулей позволяет автоматизировать процессы принятия решений по снижению потребления. С учетом того, что большая часть прогнозных данных представлена числами с плавающей точкой, предлагается использовать нечеткое сопоставление данных, нацеленное на идентификацию похожих, но не идентичных данных.

Для сопоставления данных можно использовать множество алгоритмов, включая расстояние Хэмминга, Дамерау–Левенштейна, Левенштейна. Реализация последнего из приведенных алгоритмов сводится к измерению расстояния между двумя последовательностями, цель которого – вычисление количества односимвольных правок, по формуле

$$lev(a,b) = \begin{cases} |a|, \text{ if } |b| = 0, \\ |b|, \text{ if } |a| = 0, \\ lev(tail(a), tail(b)), \text{ if } a[0] = b[0], \\ 1 + \min \begin{cases} lev(tail(a), b), \\ lev(a, tail(b)) \\ lev(tail(a), tail(b)), \end{cases} & \text{otherwise} \end{cases}$$

где $tail(x)$ – символьная строка, исключающая 1-й символ как x; $x[n]$ – символ n строки x, начинающийся с нулевой позиции.

С учетом указанной формулы возможно вычисление процентного совпадения по прогно-

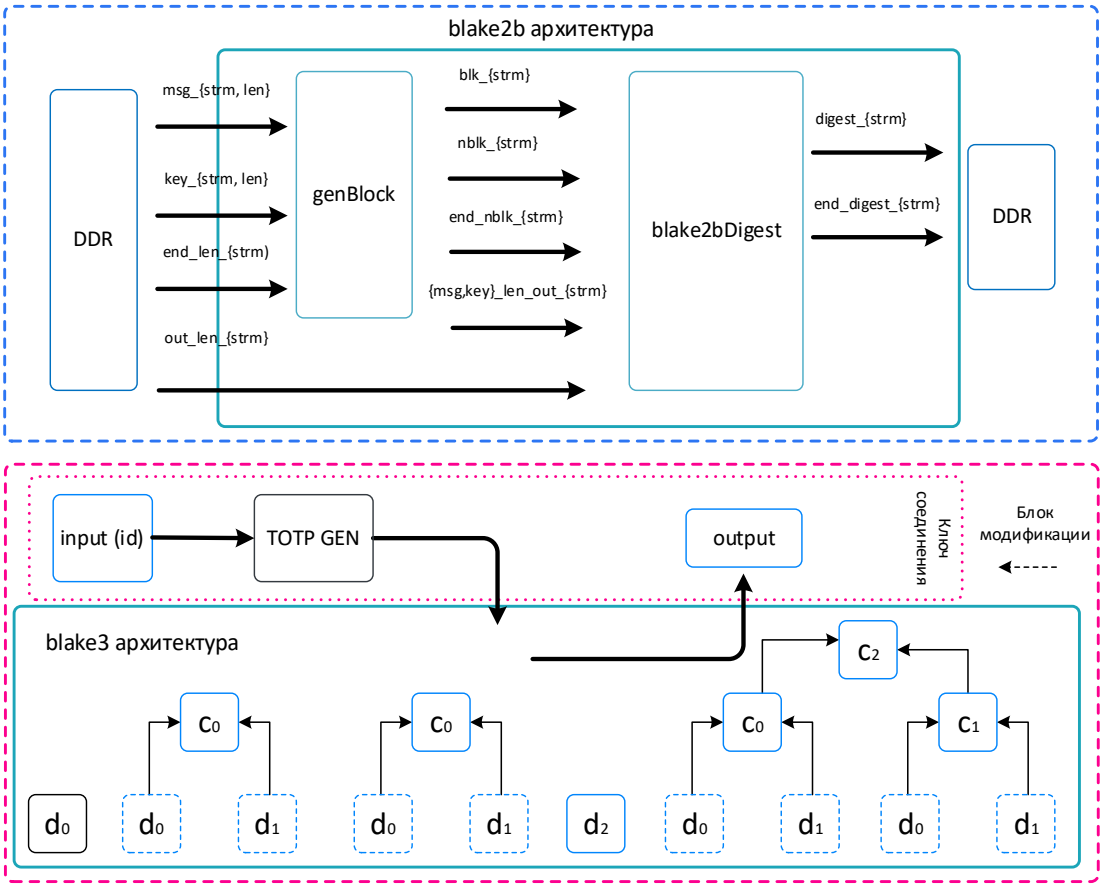

Рис. 5. Архитектуры BLAKE2B и BLAKE3 с динамическим шифрованием

Fig. 5. BLAKE2B and BLAKE3 architectures with dynamic encryption

зируемым изменениям – например, процент совпадения по 1.023 и 1.029 Mb/s (расход трафика) позволяет перераспределить приоритеты классификации для снижения нагрузки на сеть. Программная реализация указанного метода произведена с использованием библиотеки Fuzzy на языке Python, где реализованы функции как частичного, так и посимвольного сравнения [15].

Заключение

Рассмотрение инфраструктуры электросетевых компаний как единой экосистемы взаимодействия устройств в рамках TCP/IP-адресации позволило выявить существующие проблемы, такие как недостаточная эффективность при наличии множественных удаленных управляющих узлов, а также использование устаревших средств прикладного ПО и протоколов передачи данных. Для решения данных проблем в статье предложены онтологические модели классификации трафика, которые позволили разработать функциональные модули классификации и прогнозирования трафика между как локальными, так и центральными узлами сети. Для случаев несанкционированного доступа и предотвращения возможных утечек данных предлагается комбинирование средств шифрования на основе алгоритма BLAKE3 и TOTP-авторизации. Разработанный алгоритм динамического шифрования не уступает существующим алгоритмам шифрования по скорости вычисления хеш-функции и обладает поддержкой уникальности при обработке полиформатного трафика.

Существенным программным модулем в предлагаемом решении является алгоритм автоматизированного принятия решений по управлению изменениями в структуре электроэнергетических систем на основе расстояния Левенштейна. Посимвольное сравнение позволило вычислять отклонения между исходными и прогнозируемыми значениями для изменения сетевой структуры.

Список литературы

1. Васильев Д.А. Перекрестное субсидирование в электроэнергетике: текущее состояние и векторы решения проблем // Современная конкуренция. 2021. Т. 15. № 3. С. 17–30. doi: 10.37791/2687-0649-2021-15-3-17-30.

2. Склюев А.М., Хабаров В.И., Мусатова И.В., Попова О.В. Организационно-управленческие инновации в электронной промышленности России: современные тренды // Современная конкуренция. 2022. Т. 16. № 6. С. 103–116. doi: 10.37791/2687-0657-2022-16-6-103-116.

3. Zientara D. Mastering pfSense: Manage, secure, and monitor your on-premise and cloud network with pfSense 2.4. Birmingham, Packt Publ., 2018, 450 p.

4. Muthukumar M., Senthilkumar P., Jawahar M. Firewall scheduling and routing using pfSense. In: AISC, 2019, vol. 1172, pp. 749–757. doi: 10.1007/978-981-15-5566-4_67.

5. Syafei W.A., Soetrisno Y.A.A., Prasetijo A.B. Simple smart algorithm for flexibility of dynamic allocation in DHCP server for SOHO wireless router. Proc. Int. Conf. CENIM, 2020, pp. 321–325. doi: 10.1109/CENIM51130.2020.9297852.

6. Yi B., Congxiao B., Xing L. FlowLAN: A non-tunneling distributed virtual network based on IPv6. Proc. IEEE ITNEC, 2016, pp. 229–234. doi: 10.1109/ITNEC.2016.7560355.

7. Singh G.D. The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrackng, and Empire. Birmingham, Packt Publ., 2022, 742 p.

8. Бобряков А.В., Борисов В.В., Мисник А.Е., Прокопенко С.А. Моделирование и проектирование информационно-аналитических производственных процессов на основе нейронечетких темпоральных сетей Петри // Прикладная информатика. 2022. Т. 17. № 2. С. 65–78. doi: 10.37791/2687-0649-2022-17-2-65-78.

9. Yi T., Chen X., Zhu Y., Ge W., Han G. Review on the application of deep learning in network attack detection. J. of Network and Comput. Applicat., 2023, vol. 212, art. 103580. doi: 10.1016/j.jnca.2022.103580.

10. Aouini Z., Pekar A. NFStream: A flexible network data analysis framework. Comput. Networks, 2021, vol. 204, art. 108719. doi: 10.1016/j.comnet.2021.108719.

11. Пучков А.Ю., Дли М.И., Прокимнов Н.Н., Шутова Д.Ю. Многоуровневые алгоритмы оценки и принятия решений по оптимальному управлению комплексной системой переработки мелкодисперсного рудного сырья // Прикладная информатика. 2022. Т. 17. № 6. С. 102–121. doi: 10.37791/2687-0649-2022-17-6-102-121.

12. Мешалкин В.П., Дли М.И., Пучков А.Ю., Лобанева Е.И. Предварительная оценка прагматической ценности информации в задаче классификации на основе глубоких нейронных сетей // Прикладная информатика. 2021. Т. 16. № 3. С. 9–20. doi: 10.37791/2687-0649-2021-16-3-9-20.

13. Дли М.И., Синявский Ю.В., Рысина Е.И., Василькова М.А. Метод классификации перемешивающих устройств с использованием глубоких нейронных сетей с расширенным рецептивным полем // Прикладная информатика. 2022. Т. 17. № 5. С. 51–61. doi: 10.37791/2687-0649-2022-17-5-51-61.

14. Дли М.И., Булыгина О.В., Соколов А.М. Рубрицирование текстовой информации на основе голосования интеллектуальных классификаторов // Прикладная информатика. 2020. Т. 15. № 5. С. 29–36. doi: 10.37791/2687-0649-2020-15-5-29-36.

15. Дли М.И., Власова Е.А., Соколов А.М., Моргунова Э.В. Создание цифрового двойника химико-технологической системы с использованием языка Python // Прикладная информатика. 2021. Т. 16. № 1. С. 22–31. doi: 10.37791/2687-0649-2021-16-1-22-31.

Software & Systems doi: 10.15827/0236-235X.142.442-450 2023, vol. 36, no. 3, pp. 442–450

Organization of adaptive data routing in electric power complexes using ontological fuzzy classifiers

Alexander S. Fedulov
Alexey I. Lazarev

For citation
Fedulov, A.S., Lazarev, A.I., (2023) 'Organization of adaptive data routing in electric power complexes using ontological fuzzy classifiers', *Software & Systems*, 36(3), pp. 442–450 (in Russ.). doi: 10.15827/0236-235X.142.442-450
Article info
Received: 29.05.2023 After revision: 04.07.2023 Accepted: 05.07.2023

Abstract. The paper discusses the theoretical aspects of the machine learning application methods, in particular, the adaptation of deep models to the TCP/IP network topologies management in electric power complexes. The subject of the research in the paper is the author's approach to the organization of centralized network segments management in the field under consideration. The study of the interaction subjects in electric power units processes on the basis of the developed ontological models allowed to identify the main properties of multiformat data that may represent vulnerabilities for exploiting vulnerabilities. The practical significance of the research is represented by the development of a multi-module structure for tracking, classifying and predicting changes in consumed traffic, due to which it is possible to increase the efficiency of complex corporate network structures. Practical testing of existing algorithms for obtaining hash functions was carried out - the results allowed to conclude that it is advisable to use the basic BLAKE3 encryption algorithm as the main mechanism for verifying the authenticity of clients in comparison with the SHA-384, SHA-512, SHA-224, MD5

algorithms. The analytical implementation of the fuzzy character-by-character comparison algorithm as a decision-making module is given - this also allowed to confirm the relevance of the proposed approach when working with fuzzy data structures. As the main solution to these problems, an implemented approach to flexible management of the electric power plants segment represented by a complex of generating, electric grid, power supply and other companies is proposed. The main result of the proposed solution is the possible changes centralized analysis approach, taking into account adaptation to network loads based on selected ontological variables. Additional features in the implementation of this approach are compatibility with existing hardware network devices due to the unique architecture of the topology built.

Keywords: electric power systems, ontological models, data classification, decision-making, fuzzy logic, security, deep learning

Acknowledgements. This study was performed within the framework of the state assignment, project № FSWF-2023-0012

Reference List

1. Vasilyev, D. (2021) 'Cross-subsidization in the electric power industry: Current state and problem-solving vectors', *J. of Modern Competition*, 15(3), pp. 17–30 (in Russ.). doi: 10.37791/2687-0649-2021-15-3-17-30.

2. Sklyuev, A., Khabarov, V., Musatova, I., Popova, O. (2022) 'Organizational and managerial innovations in the Russian electronics industry: Current trends', *J. of Modern Competition*, 16(6), pp. 103–116 (in Russ.). doi: 10.37791/2687-0657-2022-16-6-103-116.

3. Zientara, D. (2018) *Mastering pfSense: Manage, Secure, and Monitor your On-premise and Cloud Network with pfSense 2.4*. Birmingham: Packt Publ., 450 p.

4. Muthukumar, M., Senthilkumar, P., Jawahar, M. (2019) 'Firewall scheduling and routing using pfSense', in *AISC*, 1172, pp. 749–757. doi: 10.1007/978-981-15-5566-4_67.

5. Syafei, W.A., Soetrisno, Y.A.A., Prasetijo, A.B. (2020) 'Simple smart algorithm for flexibility of dynamic allocation in DHCP server for SOHO wireless router', *Proc. Int. Conf. CENIM*, pp. 321–325. doi: 10.1109/CENIM51130.2020.9297852.

6. Yi, B., Congxiao, B., Xing, L. (2016) 'FlowLAN: A non-tunneling distributed virtual network based on IPv6', *Proc. IEEE ITNEC*, pp. 229–234. doi: 10.1109/ITNEC.2016.7560355.

7. Singh, G.D. (2022) *The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrackng, and Empire*. Birmingham: Packt Publ., 742 p.

8. Bobryakov, A., Borisov, V., Misnik, A., Prakapenka, S. (2022) 'Modeling and design of information-analytical production processes based on neuro-fuzzy temporal Petri nets', *J. of Applied Inform.*, 17(2), pp. 65–78 (in Russ.). doi: 10.37791/2687-0649-2022-17-2-65-78.

9. Yi, T., Chen, X., Zhu, Y., Ge, W., Han, G. (2023) 'Review on the application of deep learning in network attack detection', *J. of Network and Comput. Applicat.*, 212, art. 103580. doi: 10.1016/j.jnca.2022.103580.

10. Aouini, Z., Pekar, A. (2021) 'NFStream: A flexible network data analysis framework', *Comput. Networks*, 204, art. 108719. doi: 10.1016/j.comnet.2021.108719.

11. Puchkov, A., Dli, M., Prokimnov, N., Shutova, D. (2022) 'Multilevel algorithms for evaluating and making decisions on the optimal control of an integrated system for processing fine ore raw materials', *J. of Applied Inform.*, 17(6), pp. 102–121 (in Russ.). doi: 10.37791/2687-0649-2022-17-6-102-121.

12. Meshalkin, V., Dli, M., Puchkov, A., Lobaneva, E. (2021) 'Preliminary assessment of the pragmatic value of information in the classification problem based on deep neural networks', *J. of Applied Inform.*, 16(3), pp. 9–20 (in Russ.). doi: 10.37791/2687-0649-2021-16-3-9-20.

13. Dli, M., Sinyavsky, Yu., Rysina, E., Vasilkova, M. (2022) 'A method for classifying mixing devices using deep neural networks with an expanded receptive field', *J. of Applied Inform.*, 17(5), pp. 51–61 (in Russ.). doi: 10.37791/2687-0649-2022-17-5-51-61.

14. Dli, M., Bulygina, O., Sokolov, A. (2020) 'Rubrication of text information based on the voting of intellectual classifiers', *J. of Applied Inform.*, 15(5), pp. 29–36 (in Russ.). doi: 10.37791/2687-0649-2020-15-5-29-36.

15. Dli, M., Vlasova, E., Sokolov, A., Morgunova, E. (2021) 'Creation of a chemical-technological system digital twin using the Python language', *J. of Applied Inform.*, 16(1), pp. 22–31 (in Russ.). doi: 10.37791/2687-0649-2021-16-1-22-31.

Авторы

Федулов Александр Сергеевич [1], д.т.н.,
профессор, директор,
зав. кафедрой вычислительной техники,
director@sbmpei.ru
Лазарев Алексей Игоревич [1], старший лаборант,
anonymous.prodject@gmail.com

[1] Филиал Национального исследовательского университета «МЭИ» в г. Смоленске,
г. Смоленск, 214013, Россия

Authors

Alexander S. Fedulov [1], Dr.Sc. (Engineering),
Professor, Director,
Head of the Department Computer Engineering,
director@sbmpei.ru
Alexey I. Lazarev [1], Senior Laboratory Assistant,
anonymous.prodject@gmail.com

[1] Branch of the National Research University "MPEI" in Smolensk,
Smolensk, 214013, Russian Federation