

- in Large-scale Rooms. 13th *International conference on indoor air quality and climate, indoor air*, 2014, pp. 895–902. DOI: 10.13140/RG.2.1.1897.2884
11. Safonov A.A., Panfilov A.N. Application of geometric coverage algorithms for solving the problem of RFID equipment placement. *Vestnik molodjozhnoj nauki Rossii*, 2019, no. 2, pp. 39. (In Russ.)
  12. Zabelin S.L., Frolovsky V.D. Development and research of models, methods and algorithms for synthesis and analysis of solutions to geometric coating problems. *Vestnik Sibirskogo gosudarstvennogo universiteta telekommunikacij informatiki*. Novosibirsk, 2013, no 2, pp. 42–53. (In Russ.)
  13. Kureychik V.V., Glushchenko A.E. Multilevel approach for high dimensional 3D packing problem. *Izvestiya YUzhnogo federal'nogo universiteta. Tehnicheskie nauki*, 2020, no. 2 (212), pp. 6–16. (In Russ.)
  14. Valeeva A.F., Totskov I.E. Solving the problem of three-dimensional packaging. *Kompleksnyj analiz, differencial'nye uravneniya, chislennye metody i prilozheniya: materialy mezhdunarodnoj konferencii: materialy vsrossijskoj nauchno-tehnicheskoy konferencii*. Ufa: IMVC UNC RAN, 1996, pp. 30–36. (In Russ.)
  15. Verkhoturov M.A., Verkhoturova G.N. On the problem of three-dimensional packaging of objects of complex geometric shapes. *Rol' geometrii v iskusstvennom intellekte i sistemah avtomatizirovannogo proektirovaniya: materialy vsrossijskoj nauchno-tehnicheskoy konferencii*. Ulan-Ude, 1996, pp. 43–45. (In Russ.)
  16. Gil N.I. Mathematical modeling of irregular placement of planar geometric objects in design automation systems (theoretical foundations, methods, applications): avtoref. diss. ... cand. tech. sciences. Minsk, 1990, 32 p. (In Russ.)
  17. Stoyan Yu.G., Yakovlev S.V. *Mathematical models and optimization methods of geometric design*. Kiev: Sciences Dumka, 1986. 286 p. (In Russ.)
  18. Dyckhoff H. A typology of cutting and packing problems. *European Journal of Operational Research*, 1991, no. 44, pp. 145–159.
  19. Gilmore P.C., Gomory R.E. A linear programming approach to the cutting stock problem. *Operation Research*, 1961, vol. 9, no. 6, pp. 849–859.
  20. Khasanov R.I., Dyaminova E.I. Mathematical and software support for the placement of orthogonal objects in a polygonal area based on matrix technology. *Molodezhnyj vestnik Ufmskogo gosudarstvennogo aviacionnogo tehničeskogo universiteta*, 2019, no. 1 (20), pp. 183–186. (In Russ.)
  21. Yahui S., Saman H. Minimum-Cost Heterogeneous Node Placement in Wireless Sensor Networks. *IEEE Access*, 2019, vol. 7, pp. 14847–14858.
  22. Sklyar B. Digital Communication. *Theoretical foundations and practical application*. 2th Ed., revised. Moscow: Izd-vo Williams, 2007, 1104 p. (In Russ.)

Received 11.07.2023

## ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.896

### МОДЕЛИ РАСПРЕДЕЛЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПЕРСПЕКТИВНЫХ СЕТЯХ СВЯЗИ

Обухов С.А., Елагин В.С.

Санкт-Петербургский государственный университет телекоммуникаций

им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, РФ

E-mail: stasstas1155@yandex.ru

Технология 6G создаст интеллектуальную, высокомасштабируемую, динамичную и программируемую сеть беспроводной связи, способную обслуживать множество разнородных беспроводных устройств. Различные

узлы и устройства 6G будут генерировать колоссальные объемы распределенных данных, поэтому в сети пост-NGN (New Generation Networks) потребуется внедрить различные методы машинного обучения, которые позволят решать очень сложные сетевые задачи. Из-за нехватки ресурсов, ограничений по задержке и проблем с конфиденциальностью, пограничные устройства не могут выгрузить весь собранный ими набор данных на облачный сервер для централизованного обучения моделей. Для преодоления этих проблем можно использовать методы распределенного обучения, позволяющие устройствам совместно обучать модели без обмена необработанными данными, что снижает расходы на связь, задержки, а также повышает конфиденциальность данных. Модели распределенного машинного обучения будут играть важную роль в сетях 6G, они имеют ряд преимуществ перед централизованными методами, однако, реализация распределенных алгоритмов в беспроводных средах с ограниченными ресурсами может оказаться сложной задачей. Важно учитывать неопределенность беспроводной среды, связанную с большим количеством возмущающих факторов, ограниченные беспроводные (мощность передачи, радиочастотный спектр) и аппаратные (вычислительная мощность) ресурсы. Следовательно, важно выбрать правильный алгоритм машинного обучения, основанный на характеристиках беспроводной среды и требованиях к ресурсам процесса обучения. В статье рассматривается применение моделей распределенного искусственного интеллекта в коммуникационных сетях нового поколения, с целью управления ресурсами и обработки данных. Описываются основные алгоритмы и подходы распределенного машинного обучения, области применения, методы и модели. В статье анализируются способы, которыми распределенные модели искусственного интеллекта могут решать различные задачи в сетях связи, включая оптимизацию использования ресурсов и обеспечение высокой производительности и доступности сетевых сервисов.

**Ключевые слова:** машинное обучение, распределенное обучение, федеративное обучение, мультиагентное обучение, 5G, 6G, пост-NGN

## Введение

Распределенный искусственный интеллект (Distributed artificial intelligence, DAI), децентрализованный искусственный интеллект (ИИ), представляет собой область исследований ИИ, посвященную разработке распределенных решений проблем. DAI тесно связан с многоагентными системами и является их предшественником.

Системы DAI состоят из автономных узлов обработки обучения, которые могут действовать независимо. Распределенный искусственный интеллект способен решить проблемы рассуждения, планирования, обучения и восприятия искусственного интеллекта, особенно если они требуют больших объемов данных, распределяя проблему на автономные узлы обработки. Это ИИ, разнесенный на несколько компьютеров, не объединенных в общий вычислительный кластер.

DAI это тот же самый ИИ, только разнесенный на несколько компьютеров, не объединенных в единый вычислительный кластер (ни по данным, ни по приложениям, ни по доступу к отдельным компьютерам в принципе). То есть в абсолют, DAI должен быть распределен так, чтобы ни с одного из участвующих в этом «распределении» компьютеров не было возможности получить прямой доступ ни к данным, ни к приложениям других компьютеров: единственной альтернативой становится передача фрагментов данных или скриптов приложений через «явные» сообщения. Любые отступления от этого абсолюта, по идее, приводят к возникновению «частично распределенного искусственного интеллекта» – например, данные распределены, а сервер приложений об-

щий. Или наоборот. Так или иначе, мы получаем на выходе набор «федерированных» моделей (т. е. либо обученных каждая на своем источнике данных, либо обученных каждая своим алгоритмом, либо «и то и другое вместе»).

## Обзор предметной области

Быстрый рост объема данных и доступности информации в последние годы привел к изменению парадигмы (набора концепций и шаблонов) в беспроводных сетях: большими данными (big data) больше нельзя управлять как единым целым. Следует предусмотреть новые распределенные малые данные (small data), когда большие объемы данных распределяются между несколькими узлами для их обработки [1].

Стандарт 6G обеспечит подключение по всему миру, уменьшит задержку и позволит расширять приложения, основанные на чрезвычайно плотных и разнообразных беспроводных сетях, таких как системы Интернета вещей (Internet of Things, IoT) [2].

Интеллектуальное взаимодействие между устройствами по всей сети является целью разработки методов распределенного машинного обучения (Distributed Machine Learning, DML). DML будет иметь важное значение для управления и эксплуатации постоянно увеличивающегося объема данных и коммуникаций в межмашинном взаимодействии (machine to machine) в сетях, которые находятся не в оптимальных условиях. В таких приложениях нет необходимости отправлять большие объемы данных в центральную систему, которая создает обучающую модель. Вместо этого, обработкой данных и локальными наблюдени-

ями занимаются сами устройства на границе сети. Такие решения имеют различные преимущества: значительное снижение нагрузки на передачу данных, возможность оптимизации использования ресурсов, а также экономия средств [3].

В отличие от предыдущих поколений, беспроводные сети 5G, добиваются существенных улучшений в задержке, скорости передачи данных, мобильности и количестве подключенных устройств. Сеть 5G с интегрированными технологиями, такими как IoT, mobile edge computing (MEC), fog computing и machine learning (ML), охватывает различные сферы жизни общества, включая робототехнику, автомобильные сети, здравоохранение. По прогнозам, сети 5G достигнут своего предела через десятилетие, поэтому, ученые и органы по стандартизации уже работают над созданием нового поколения беспроводной связи, получившего название 6G [4; 5].

Ключевые технические задачи для сетей 6G [6]:

- сверхвысокая скорость передачи данных (до 1 Тбит/с);
- сверхнизкая задержка;
- высокая энергоэффективность для устройств с ограниченными ресурсами;
- покрытие сети по всему миру;
- надежное и интеллектуальное подключение по всей сети.

Спектр потребностей приложений 6G будет охватывать широкий диапазон пропускной способности, задержек, надежности, масштабируемости, доступности услуг, непрерывности обслуживания и аспектов безопасности. Одновременно достижение значительно более высокой ресурсоэффективности, чем в 5G, является важным шагом не только к расширению пропускной способности спектра, но и к достижению амбициозных целей по снижению энергопотребления для будущих сетей. В результате конструкция радиодоступа 6G должна быть гибкой и ресурсоэффективной, с возможностью корректировки в режиме реального времени [7].

Поддержка требований широкого спектра приложений и вариантов использования 6G является серьезной задачей. Для поддержки таких новых технологических достижений необходимо обеспечить гораздо более высокий уровень интеллекта, и приложить больше усилий по обработке данных. Поэтому искусственный интеллект (Artificial Intelligence, AI) и ML рассматриваются как фундаментальные элементы грядущих сетей 6G, а не просто как инструмент оптимизации для оценки производительности.

Однако, большинство современных решений

AI и ML используют централизованное обучение (centralized learning, CL), при котором данные собираются по всей системе, но обучение выполняется в одном месте. CL не является идеальным, часто бывает слишком дорогостоящим на распределенной платформе, в сетях операторов связи. В централизованном центре обработки данных существуют значительные требования к энергоснабжению, которые должны покрываться ответственным арендатором/владельцем, а также соображения конфиденциальности [7].

В результате, по мере приближения к внедрению сетей 6G, будет крайне важно разработать новые процедуры, которые позволят системе функционировать должным образом, а также координировать обучение и распределение вычислительных, сетевых, накопительных (ресурсы хранилищ) и энергетических ресурсов.

С инженерной точки зрения, способность управлять чрезвычайно разнообразными ресурсами, динамичность системы и эффективное обучение в режиме реального времени являются основными препятствиями для достижения такого рода технологического развития. С другой стороны, в области алгоритмики будущие объективные решения будут включать возможность выполнять обучение с использованием сильно фрагментированных данных, small data, повышать эффективность в динамичных средах и управлять агентами передачи совместного обучения (AI-powered collaborative learning) с целью оптимизации обработки аномалий.

### **Алгоритмы распределенного машинного обучения**

С развитием стандарта беспроводной связи 5G в сетевые инфраструктуры интегрируется большой набор разнородных устройств с датчиками, возможностями хранения и обработки данных. Эти устройства могут собирать терабайты данных, которые могут быть использованы для анализа и решения различных сетевых задач. Для этих операций могут быть полезны различные алгоритмы ML.

При традиционных централизованных подходах к ML, данные, собранные устройствами, должны передаваться на централизованный узел, оснащенный более мощными возможностями обработки. Однако, ресурсы беспроводных устройств могут быть ограничены, и такой подход может оказаться сложным, особенно в случае приложений и служб, требовательных к низким задержкам. Кроме того, пользователи сети становятся все более осведомленными о конфиденци-

альности и неохотно делятся своими конфиденциальными данными с внешним миром, чтобы избежать потенциальной кражи данных.

Благодаря недавнему прогрессу в аппаратных и программных технологиях, устройства могут обрабатывать ограниченный набор данных на борту (onboard), что позволяет им создавать локальные модели ML на основе своих данных, однако, точность таких моделей ограничена.

Интегрируя локальные вычислительные устройства и возможности централизованной обработки данных, можно реализовать различные методы deep learning (DL) и федеративного обучения (federated learning, FL) [8].

Кроме того, сетевые настройки, основанные на облачных вычислениях, все чаще заменяются обработкой на границе сети, то есть пограничными вычислениями (edge computing AI), что позволяет реализовать алгоритмы ML для наилучшего использования данных, генерируемых этими устройствами [8; 9].

Таким образом, в перспективных сетях связи, концепция централизованного ML больше не является доминирующей.

В основе новой тенденции лежит внедрение алгоритмов DL, таких как FL и мультиагентное обучение с подкреплением (multi-agent reinforcement learning, MARL).

### **Федеративное, объединенное обучение**

Федеративное, объединенное обучение (FL, также известное как совместное обучение) – это метод ML, который обучает алгоритм с помощью нескольких независимых сеансов, каждый из которых использует свой собственный набор данных. Этот подход отличается от традиционных централизованных методов машинного обучения, при которых локальные наборы данных объединяются в один учебный сеанс, а также от подходов, предполагающих, что локальные выборки данных распределены идентично.

FL позволяет нескольким участникам создавать общую, надежную модель ML без совместного использования данных, решая таким образом такие важнейшие проблемы, как обеспечение конфиденциальности данных, безопасности данных, права доступа к данным, порядок доступа к разнородным данным. Приложения FL применяются в отраслях телекоммуникации и IoT.

FL направлено на обучение алгоритма ML, например, глубоких нейронных сетей (deep neural networks), на нескольких локальных наборах данных, содержащихся в локальных узлах, без явного обмена выборками данных. Общий принцип

заключается в обучении локальных моделей на локальных выборках данных и обмене параметрами (например, весами и смещениями глубокой нейронной сети) между этими локальными узлами с некоторой частотой для генерации глобальной модели, общей для всех узлов [10].

Основное различие между FL и DL заключается в предположениях, сделанных относительно свойств локальных наборов данных, поскольку DL изначально направлено на распараллеливание вычислительной мощности, в то время как FL изначально направлено на обучение на разнородных наборах данных. Хотя DL также направлено на обучение одной модели на нескольких серверах, общим базовым предположением является то, что локальные наборы данных независимы, распределены одинаково и имеют примерно одинаковый размер. Ни одна из этих гипотез не выдвигается для FL, вместо этого наборы данных, как правило, неоднородны, и их размеры могут варьироваться на несколько порядков. Более того, клиенты, участвующие в FL, могут быть ненадежными, поскольку они подвержены большему количеству сбоев или выбывают из системы, поскольку они обычно полагаются на менее мощные средства связи (например, Wi-Fi) и системы с батарейным питанием (например, смартфоны и устройства IoT) по сравнению с DL, где узлами обычно являются центры обработки данных с мощными вычислительными возможностями и соединены друг с другом быстрыми сетями [11].

Компания Google предложила концепцию FL в 2016 году. Учитывая огромный объем данных, доступных в настоящее время в сети, концепция состоит в том, чтобы построить модели ML на основе наборов данных, распределенных по большому количеству устройств, избегая при этом разброса данных.

Цель этой стратегии – предоставить пользователям преимущества наличия огромного объема доступных данных без необходимости их централизованного хранения.

Обычно все данные от  $N$  владельцев группируются вместе и используются для обучения модели. В системах FL каждому владельцу данных не нужно предоставлять свои данные другим пользователям.

### **Мультиагентное обучение с подкреплением**

Мультиагентное обучение с подкреплением (MARL) – это подотрасль обучения с подкреплением. Она фокусируется на изучении поведения множества обучающихся агентов, которые сосу-

ществуют в общей среде. Каждый агент мотивирован своими собственными вознаграждениями и совершает действия для продвижения своих собственных интересов. В некоторых средах эти интересы противоположны интересам других агентов, что приводит к сложной групповой динамике.

Различные проблемы беспроводной связи могут быть смоделированы как проблемы последовательного принятия решений и могут быть эффективно решены с помощью подходов, основанных на RL.

В большинстве беспроводных сред требуется настройка нескольких агентов, чтобы они могли взаимодействовать друг с другом и влиять на процессы принятия решений друг другом.

Поэтому MARL является потенциальным кандидатом для решения различных задач последовательного принятия решений в различных беспроводных средах, благодаря разработкам методов функциональных приближений, исследованиям операций в многоагентных системах [12].

Настройки MARL можно разделить на три основные группы, основанные на взаимодействии агентов друг с другом.

В первом случае, полностью кооперативных настроек MARL, все агенты могут работать сообща над оптимизацией общей цели или сигналов вознаграждения. В этой ситуации агенты обычно получают аналогичные вознаграждения [13].

Во втором случае, полностью конкурентных настроек MARL, все агенты могут конкурировать друг с другом, каждый агент эгоистично пытается максимизировать свое вознаграждение. Следовательно, общая сумма значений вознаграждения для всех агентов, участвующих в процессе обучения, может быть равна нулю [13].

Существуют также гибридные системы MARL, в которых могут присутствовать как кооперативные, так и конкурирующие агенты.

### Основные области применения DL

Основные области применения методов DL:

1. Наземные сети (Non-terrestrial networks, NTN).

Недавно в наземные сетевые системы были интегрированы различные новые наземные сетевые платформы, чтобы увеличить доступное количество ресурсов, решить проблемы, связанные с безопасностью, и придать гибкость и большую устойчивость каналам связи.

Различные методы DL нашли свое применение в NTN, такие как приложения, включающие совместное использование спектра, проектирование траекторий, оптимизацию трафика, безопасность, а также распределение задач и ресурсов [4].

23 февраля 2023 года компания *Samsung Electronics* объявила о создании системы «5G NTN», которая обеспечит возможность непосредственного обмена информацией между смартфонами и спутниками.

Для поддержания высоконадежной связи со спутниками на низкой околоземной орбите будет использоваться аппаратная платформа Euphros Modem 5300, соответствующая стандарту «3GPP Release 17». Платформа функционально совместима с решениями, предлагаемыми глобальными операторами связи, производителями мобильных устройств, поставщиками чипов. Предполагается поддержка технологий DAI и DL, чтобы ускорить спутниковую связь 5G и продолжить путь к эре 6G.

2. Автомобильные самоорганизующиеся сети (Vehicular ad-hoc network, VANET).

Методы DL широко используются для решения сложных задач в VANET. Основные области применения включают интеллектуальное обнаружение объектов, распределение сетевых ресурсов, обмен данными с транспортными средствами, разгрузку вычислений в системах с поддержкой периферийных вычислений, управление светофорами [14].

3. Энергетические системы (Power systems).

В последнее время для решения проблем, связанных с энергосистемой, используются различные методы DL. Основные области энергосистем, где используются методы DL: регулирование напряжения, управление энергопотреблением, прогнозирование спроса, повышение стабильности в переходных процессах и отказоустойчивости [15].

4. Сети электронного здравоохранения (E-health).

Системы E-health наполняются различными новыми приложениями с высокой вычислительной сложностью и требованиями к ресурсам. Различные методы DL нашли применение в системах E-health [16].

Учитывая конфиденциальный характер медицинских данных, подходы FL, обеспечивающие сохранение конфиденциальности, вызвали большой интерес. Последние достижения в области технологии FL применимы к E-health, особенно для Интернета медицинских вещей (Internet of Medical Things, IoMF). Предполагается создание многослойной платформы FL, защищающей конфиденциальность IoMF.

### DML в сетях 6G

AI играет ключевую роль в определении видения будущих технологий 6G. Методы ML, в частности DML, могут сыграть важную роль в технологии 6G в 2030-х годах.

В этом разделе будут рассмотрены и проанализированы некоторые методы DML, применяемые в области телекоммуникаций.

Существует глобальная модель ML, основанная на традиционной методике (Federated Averaging Algorithm, FedAvg), которая была описана ранее. Она используется в случае, если все устройства имеют независимые и идентично распределенные наборы данных (Independent and Identically Distributed Data, IID).

Однако на практике, в системах с беспроводной связью и разнородными узлами, традиционные FL системы на базе IID имеют ограниченную производительность, они не подходят для применения в области беспроводных сетей.

Учитывая это, группы ученых (*Chen M., Gündüz D., Huang K., Saad W., Bennis M., Feljan A.V., Poor H.V.*) в научной статье «*Distributed Learning in Wireless Networks: Recent Progress and Future Challenges*» предложили два усовершенствованных алгоритма FL: объединенное многозадачное обучение (federated multi-task learning, FMTL) и FL на основе метаобучения, не зависящего от модели (model agnostic meta-learning, MAML) [3].

В случае FMTL, задача минимизации определяется как:

$$\min_{M, \Omega} \sum_{i=1}^U \sum_{k \in K_i} f(m_i, x_{i,k}, y_{i,k}) + R(M, \Omega), \quad (1)$$

где  $M = [m_1, m_2, \dots, m_U]$ ;  $\Omega$  – моделирует взаимосвязь между различными операциями обучения устройства;  $R$  – функция регулирования.

Задачу можно разделить на подзадачи, чтобы предоставить устройствам возможность работать распределенным образом для достижения поставленной цели. Все устройства в FedAvg используют одну и ту же модель конвергенции (convergence), однако, в случае FMTL, устройства могут иметь разную сходимость (convergences), поскольку одна модель может иметь меньшие потери при обучении, чем другая, из-за распределения, отличного от IID [3].

Методика FL, основанная на MAML, пытается разработать модель ML, которая позволяет каждому устройству создать свою собственную модель после нескольких «итераций градиентного спуска» (используется метод Stochastic Gradient Descent, SGD).

Градиентный спуск (GD) – это итеративный алгоритм оптимизации первого порядка, используемый для нахождения локального минимума / максимума заданной функции. GD используется в ML и DL для минимизации функции затрат/потерь, например, в линейной регрессии.

В этой ситуации задача формулируется следующим образом:

$$\min_m \sum_{i=1}^U \frac{P_i}{k_i} \sum_{k \in K_i} f(m - \lambda \nabla f_i, x_{i,k}, y_{i,k}), \quad (2)$$

где  $\nabla f_i$  – градиент снижения локальной ML модели  $i$ -го устройства;  $\lambda$  – скорость обучения.

Основные характеристики подходов FMTL и MAML:

1. Алгоритм FMTL напрямую оптимизирует локальную модель каждого устройства, в то время как MAML оптимизирует исходную модель всех устройств.

2. При работе с данными IID необходим алгоритм FedAvg. FMTL и MAML более практичны для данных, не относящихся к IID.

3. Сервер параметров (parameter server, PS) должен знать о распределении данных в устройствах, чтобы выбирать между FMTL и MAML.

4. Все алгоритмы FL должны обучаться с помощью распределенного итеративного процесса (distributed iterative algorithms).

### Показатели производительности FL в беспроводных сетях

Для оценки эффективности реализации FL в беспроводных сетях используются четыре ключевых показателя: 1) потери при обучении (training loss); 2) время конвергенции, сходимости (convergence time, T); 3) потребление энергии; 4) надежность [17].

1) Потери при обучении – это значение функции потерь ( $f$ ), которая используется в формулах (1) и (2). Модели устройств ML передаются по несовершенным соединениям в беспроводных сетях, следовательно, возможны проблемы с передачей, которые могут серьезно влиять на потери при обучении. Кроме того, из-за ограниченной энергии и вычислительной мощности, только небольшое подмножество устройств может активно участвовать в процессе обучения, в результате чего только часть моделей ML используется для построения глобальной модели, и это также приводит к негативным последствиям [4].

2) Время сходимости для реализаций FL в беспроводных сетях выражается как [4]:

$$T = (T_c + T_T) \times N_T, \quad (3)$$

где  $T_c$  – время, необходимое каждому устройству для обновления своей локальной модели на каждом шаге обучения;

$T_T$  – максимальное время передачи данных на каждом шаге обучения;

$N_T$  – количество шагов обучения, необходимое для конвергенции, сходимости FL.

Из (3) видно, что  $T$  FL зависит от трех компонентов: 1) задержки передачи параметров ML  $T_T$ ; 2) времени  $T_c$ , необходимого каждому устройству для обучения своей локальной модели ML; 3) количества шагов обучения  $N_T$ .

Оба фактора  $N_T$  и  $T_c$  являются зависимыми. Увеличение количества шагов SGD для обновления локальной модели на каждом этапе обучения (например, за счет увеличения  $T_c$ ) может уменьшить количество шагов, необходимых FL для сходимости.

3) Энергопотребление ( $E$ ) каждого устройства, участвующего в обучении FL, выражается как [4]:

$$E = (E_c + E_T) \times N_T, \quad (4)$$

где  $E_c$  – энергия, потребляемая каждым устройством во время обучения его модели на каждом шаге обучения;

$E_T$  – энергия, необходимая для передачи параметров ML на PS на каждом этапе;

$N_T$  – количество шагов обучения, необходимое для конвергенции, сходимости FL.

Из (4) видно, что энергопотребление каждого устройства зависит от трех компонентов: 1) энергопотребления для передачи параметров ML; 2) энергопотребления для обучения локальной модели ML; 3) количества шагов обучения, которое необходимо FL для сходимости.

4) Надежность FL определяется как вероятность того, что FL достигнет определенного (целевого) значения потерь при обучении. Устройства, которые фактически участвуют в каждой фазе обучения, являются подмножеством общего числа устройств, поэтому устройства и передающиеся параметры могут меняться на каждом этапе. Это может повлиять на  $T$  и потери [4].

### Влияние характеристик беспроводной связи на показатели FL

Характеристики беспроводной сети, такие как спектр, мощность передачи и вычислительная мощность, влияют на показатели FL, обозначенные в предыдущем разделе [4].

В таблице 1 обобщена взаимосвязь между различными характеристиками беспроводной связи

и показателями производительности FL. Символ «+» означает, что изменение параметра связи повлияет на показатели производительности FL.

Например, ресурс спектра, выделенный каждому устройству для передачи параметров FL, будет влиять на потери при обучении. Время передачи параметров FL на шаг обучения  $T_c$ , потребление энергии при передаче параметров FL  $E_c$  и надежность FL.

Таким образом, на основе данных из таблицы 1, чтобы дать оценку эффективности реализации FL, можно описать взаимосвязь характеристик беспроводных сетей и показателей FL.

На производительность FL влияют факторы беспроводной связи, в частности, спектральные ресурсы, выделенные на каждом устройстве, определяют отношение сигнала к помехам и шуму (signal to interference-plus-noise ratio, SINR), скорость передачи данных и вероятность того, что параметр содержит ошибки. В результате они оказывают влияние на потери при обучении, TT, ET и надежность обучения [18].

Количество обновлений метода SGD, которые могут быть сделаны для каждого этапа обучения, определяется вычислительной мощностью. В результате это влияет на количество времени и энергии, затрачиваемых на локальное обучение. В то же время, уменьшение количества обновлений SGD увеличит потери при обучении и количество шагов, необходимых для сходимости FL.

Таким образом, SINR, скорость передачи данных и вероятность включения ошибок при передаче параметров – все это определяется мощностью передачи и беспроводным каналом. В результате увеличение мощности передачи каждого устройства снижает потери, TT, NT и надежность при одновременном увеличении ET.

В FL потери при обучении и NT уменьшаются по мере увеличения числа участников, в то время как TT и надежность повышаются.

Потери при обучении, надежность и общее количество этапов обучения могут уменьшаться по мере увеличения количества параметров FL, обучаемых каждым устройством. Однако количество

Таблица 1. Влияние характеристик беспроводной связи на показатели FL

Характеристика	Потеря передачи	$T_c$	$T_T$	$N_T$	$E_c$	$E_T$	Надежность
Спектральный ресурс	+		+	+		+	+
Вычислительная мощность	+	+		+	+		
Мощность передачи	+		+	+		+	+
Беспроводной канал	+		+	+		+	+
Набор устройств, участвующий в FL	+		+	+			+
Размер параметров FL обученных каждым устройством	+	+		+	+		+
Размер параметров FL передаваемых каждым устройством			+			+	

энергии и времени, затрачиваемых на обучение модели, возрастет.

### Заключение

Несмотря на то, что в сетях 6G могут быть реализованы значительные вычислительные мощности и широкополосная передача данных, задержки и проблемы с пропускной способностью могут по-прежнему мешать обучению моделей на больших объемах данных. В этом контексте распределенные подходы машинного обучения становятся крайне важным инструментом для обработки больших объемов данных.

Одним из преимуществ DML является возможность обработки больших объемов данных, которые будут генерироваться в сетях 6G, без необходимости передачи их на центральный сервер. Это позволяет сохранять конфиденциальность данных и уменьшать нагрузку на сеть.

В сетях 6G могут использоваться различные подходы к ML, FL, MARL, а также различные методы, включая метод средних скользящих, метод минимального фрагмента, метод линейной регрессии. Каждый из этих методов имеет собственные преимущества и ограничения, которые должны быть учтены при выборе метода для конкретной задачи. Распределенные методы могут помочь ускорить обучение, снизить задержки, улучшить производительность. DML способно обеспечить более быстрый доступ к данным и лучшие показатели энергопотребления в сетях 6G.

FL позволит обучать модели на данных, которые хранятся на разных устройствах, без необходимости передачи этих данных на центральный сервер. То есть, несколько устройств смогут «сотрудничать» в задаче ML, не раскрывая свои данные, обеспечивая конфиденциальность и безопасность.

MEC позволят выполнять обработку данных ближе к источнику, снижая задержку и уменьшая нагрузку на центральный сервер, что улучшит эффективность сети.

Подходы на основе блокчейна могут улучшить безопасность и прозрачность DML, предоставляя децентрализованную и невозможную для подделки среду для обмена и обработки данных.

MARL может быть использовано для создания автономных систем, которые могут принимать решения на основе полученных данных.

Комбинация этих методов может позволить сетям 6G обрабатывать огромные объемы данных в режиме реального времени и поддерживать различные приложения, такие как NTN, VANET умные города и E-health. Это может привести к

более эффективному использованию ресурсов сети и улучшению качества жизни людей.

Таким образом, разработка распределенных алгоритмов ML является важным направлением исследований для создания эффективных и масштабируемых 6G сетей.

### Литература

1. Saad W., Bennis M., Chen M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems // *IEEE Network*. 2020. Vol. 34, no. 3. P. 134–142.
2. 6G Wireless Communications: Vision and Potential Techniques / P. Yang [et al.] // *IEEE Network*. 2019. Vol. 33, no. 4. P. 70–75.
3. Distributed Learning in Wireless Networks: Recent Progress and Future Challenges / M. Chen [et al.] // *IEEE Journal on Selected Areas Communications*. 2021. Vol. 39. P. 3579–3605.
4. Muscinelli E., Shinde S. S., Tarch D. Overview of Distributed Machine Learning Techniques for 6G Networks // *Algorithms*. 2022. Vol.15. P. 210:1–210:28.
5. Елагин В.С., Богачев А.В., Белозерцев И.А. Модель оценки сквозной задержки пакетов для цепочки NFV узлов в сетях пятого поколения // *T-Comm: Телекоммуникации и транспорт*. 2022. Т. 16, № 3. С. 23–30.
6. A Survey on Green 6G Network: Architecture and Technologies / T. Huang [et al.] // *IEEE Access*. 2019. Vol. 7. P.175758–175768.
7. Bishoyi P.K., Misra S. Enabling Green Mobile-Edge Computing for 5G-Based Healthcare Applications // *IEEE Transactions Green Communications Networking*. 2021. Vol. 5, no. 3. P. 1623–1631.
8. Distributed machine learning for multiuser mobile edge computing systems / Y. Guo [et al.] // *IEEE Journal of Selected Topics in Signal Processing*. 2022. Vol. 16, no. 3. P. 460–473.
9. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications / A. Vladyko [et al.] // *Electronics*. 2022. Vol. 11. P. 3–4. DOI 10.3390/electronics11020173.
10. Communication-Efficient Learning of Deep Networks from Decentralized Data / H.B. McMahan [et al.] // *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*. Ft. Lauderdale, USA, 2017. Vol. 54. P. 1273–1282.
11. Federated Machine Learning: Concept and Applications / Q. Yang [et al.] // *ACM Transactions*

- on Intelligent Systems Technologies. 2019. Vol. 10, no. 2. P. 12:1–12:19.
12. Feriani A., Hossain E. Single and multi-agent deep reinforcement learning for AI-enabled wireless networks: A tutorial // *IEEE Communications Surveys and Tutorials*. 2021. Vol. 23, no. 2. P. 1226–1252.
  13. Zhang K., Yang Z., Basar T. Multi-Agent Reinforcement Learning: A Selective Overview of Theories and Algorithms: *Handbook of Reinforcement Learning and Control*. Switzerland, Cham: Springer, 2021. P. 321–384.
  14. Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles / X. Zhou [et al.] // *IEEE Transactions on Vehicular Technology*. 2021. Vol. 70. P. 5308–5317.
  15. Gholizadeh N., Musilek P. Distributed learning applications in power systems: A Review of Methods, Gaps, and Challenges // *Energies*. 2021. Vol. 14. P. 3654.
  16. Bishoyi P.K., Misra S. Towards Energy-and Cost-Efficient Sustainable MEC-Assisted Healthcare Systems // *IEEE Transactions on Sustainable Computing*. 2022. Vol. 7, no. 2. P. 550–556.
  17. Providing QOS for OTT Services in Communication Networks / A.B. Goldstein [et al.] // *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*. Moscow: Institute of Electrical and Electronics Engineers, 2020. P. 9078633. DOI: 10.1109/IEEECONF48371.2020.9078633

*Получено 30.08.2023*

**Обухов Станислав Андреевич**, аспирант кафедры инфокоммуникационных систем (ИКС) Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ). 193232, Российская Федерация, г. Санкт-Петербург, пр. Большевиков, 22, к. 1. Тел. +7 996 798-46-08. E-mail: stasstas1155@yandex.ru

**Елагин Василий Сергеевич**, к.т.н., доцент кафедры ИКС СПбГУТ. 193232, Российская Федерация, г. Санкт-Петербург, пр. Большевиков, 22, к. 1. Тел. +7 812 326-31-63 (2100). E-mail: v.elagin@spbgut.ru

## DISTRIBUTED ARTIFICIAL INTELLIGENCE MODELS IN PERSPECTIVE COMMUNICATION NETWORKS

*Obukhov S.A., Elagin V.S.*

*The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,  
Saint Petersburg, Russian Federation*

*E-mail: stasstas1155@yandex.ru*

6G technology will create an intelligent, highly scalable, dynamic and programmable wireless network capable of serving a variety of heterogeneous wireless devices. Various 6G modules and devices will generate colossal amounts of distributed data, so post-NGN (New Generation Networks) will need to implement a number of machine learning methods that will solve significantly complicated network problems. To overcome these problems, distributed learning methods can be used, allowing devices to train models jointly, without exchanging raw data, which reduces communication costs, delays, and increases data privacy level as well. Distributed machine learning models will play an important role in 6G networks, since they have a number of advantages over centralized methods, however, the implementation of distributed algorithms in resource-constrained wireless environments can be challenging. It is important to take into account the wireless environment uncertainty associated with various disturbing factors and limited wireless (transmission power, radio frequency spectrum) and hardware resources (computing power). Consequently, it is important to choose the suitable machine learning algorithm based on the wireless environment characteristics and the resource requirements of the learning process. The article reviews the application of distributed artificial intelligence models in new generation communication networks for resource management and data processing purposes. The general algorithms and approaches of distributed machine learning, applications, methods and models are described. The article analyzes the ways in which distributed artificial intelligence models can solve various problems in communication networks, including optimizing resource use and ensuring high performance and availability of network services.

**Keywords:** machine learning, distributed learning, federated learning, multi-agent learning, 5G, 6G, post-NGN

**DOI:** 10.18469/ikt.2023.21.1.08

**Obukhov Stanislav Andreevich**, Bonch-Bruевич Saint Petersburg State University of Telecommunications, 22, building 1, Bolshevikov Avenue, Saint Petersburg, 193232, Russian Federation; PhD Student of the Department of Infocommunication Systems. Tel. +7 996 798-46-08. E-mail: stasstas1155@yandex.ru

**Elagin Vasily Sergeevich**, Bonch-Bruевич Saint Petersburg State University of Telecommunications, 22, building 1, Bolshevikov Avenue, Saint Petersburg, 193232, Russian Federation; Associate Professor of Infocommunication Systems Department, PhD in Technical Science. Tel. +7 812 326-31-63 (2100). E-mail: v.elagin@spbgut.ru

## References

1. Saad W., Bennis M., Chen M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network*, 2020, vol. 34, no. 3. pp. 134–142.
2. Yang P. et al. 6G Wireless Communications: Vision and Potential Techniques. *IEEE Network*, 2019, vol. 33, no. 4, pp. 70–75.
3. Chen M. et al. Distributed Learning in Wireless Networks: Recent Progress and Future Challenges. *IEEE Journal on Selected Areas Communications*, 2021, vol. 39, pp. 3579–3605.
4. Muscinelli E., Shinde S.S., Tarch D. Overview of Distributed Machine Learning Techniques for 6G Networks. *Algorithms*, 2022, vol. 15, pp. 210:1–210:28.
5. Elagin V.C., Bogachov A.V., Belozertsev I.A. Modeling the estimation of end-to-end packet latency for a chain of NFV nodes in 5G networks. *T-Comm: Telecommunication and Transport*, 2022, vol.16, no. 3, pp. 23–30. (In Russ.)
6. Huang T. et al. A Survey on Green 6G Network: Architecture and Technologies. *IEEE Access*, 2019, vol. 7, pp. 175758–175768.
7. Bishoyi P.K., Misra S. Enabling Green Mobile-Edge Computing for 5G-Based Healthcare Applications. *IEEE Transactions Green Communications Networking*, 2021, vol. 5, no. 3, pp. 1623–1631.
8. Guo Y. et al. Distributed machine learning for multiuser mobile edge computing systems. *IEEE Journal of Selected Topics in Signal Processing*, 2022, vol. 16, no. 3, pp. 460–473.
9. Vladyko A. et al. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications. *Electronics*, 2022, vol. 11, pp. 3–4. DOI 10.3390/electronics11020173.
10. McMahan H.B. et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*. Ft. Lauderdale, USA, 2017, vol. 54, pp. 1273–1282.
11. Yang Q. et al. Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems Technologies*, 2019, vol. 10, no. 2, pp. 12:1–12:19.
12. Feriani A., Hossain E. Single and multi-agent deep reinforcement learning for AI-enabled wireless networks: A tutorial. *IEEE Communications Surveys & Tutorials*, 2021, vol. 23, no. 2, pp.1226–1252.
13. Zhang K., Yang Z., Basar T. *Multi-Agent Reinforcement Learning: A Selective Overview of Theories and Algorithms: Handbook of Reinforcement Learning and Control*. Switzerland, Cham: Springer, 2021, pp. 321–384.
14. Zhou X. et al. Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles. *IEEE Transactions on Vehicular Technology*, 2021, vol. 70, pp. 5308–5317.

15. Gholizadeh N., Musilek P. *Distributed learning applications in power systems: A Review of Methods, Gaps, and Challenges*. *Energies*, 2022, vol. 14, pp. 3654.
16. Bishoyi P.K., Misra S. Towards Energy-and Cost-Efficient Sustainable MEC-Assisted Healthcare Systems. *IEEE Transactions on Sustainable Computing*, 2022, vol. 7, no. 2, pp. 550–556.
17. Goldstein A.B. et al. Providing QOS for OTT Services in Communication Networks. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*. Moscow: Institute of Electrical and Electronics Engineers, 2020, pp. 9078633. DOI: 10.1109/IEECONF48371.2020.9078633.

Received 30.08.2023

## НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3.07

### МЕТОДЫ И СРЕДСТВА КВАНТОВОЙ КРИПТОГРАФИИ

Васин Н.Н.

Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ

E-mail: vasin-nn@psuti.ru

Для обеспечения безопасного обмена данными по сети необходимо соблюдать требования к конфиденциальности, целостности и доступности передаваемой информации. Для соблюдения указанных требований производится шифрование данных на передающей стороне и дешифрование полученной информации – на принимающей стороне. Шифрование передаваемого сообщения выполняется по правилам, которые определяются алгоритмом и ключом. Криптобезопасность зашифрованной информации зависит от длины ключа. Среди алгоритмов шифрования выделяют алгоритмы с симметричным (закрытым) ключом и с асимметричным (открытым) ключом. При всех достоинствах закрытого ключа для его доставки от одного пользователя другому (распределение ключей) используют асимметричные ключи. Однако высокопроизводительные квантовые компьютеры способны дешифровать перехваченную информацию. Поэтому в современных криптографических системах используют квантовое распределение ключей. Идея использования квантовых битов была предложена в 1970 г. С. Визнером. В 1984 г. Ч. Беннет и Ж. Brassar предложили протокол BB84. Использование «запутанных» квантов для систем с квантовым распределением ключей предложил в 1991 г. А. Экерт. На основе указанных протоколов создаются все современные системы квантовой криптографии.

**Ключевые слова:** передача информации, криптография, квантовое распределение ключей, поляризация, протоколы (алгоритмы) шифрования BB84, B92, E91, BBM92, запутанные кванты

#### Введение

Безопасный обмен сообщениями по сети обеспечивается с помощью алгоритмов и ключей шифрования. Чем длиннее ключ, тем труднее его взломать, т.к. на это тратится больше вычислительных ресурсов. Для безопасного распределения ключей разработан целый ряд протоколов [1].

Среди множества классических алгоритмов (протоколов) шифрования можно выделить два типа: с симметричным (закрытым, секретным) ключом и с асимметричным (открытым) ключом, что позволяет компьютерам совместно использовать ресурсы сети [1–3].

В первом случае передающая и принимающая сторона имеют одинаковый ключ, который нужно заблаговременно доставить обеим сторонам обмена данными. Недостатком алгоритма является сложность доставки ключей множеству взаимо-

действующих пар абонентов по открытым каналам связи (сложность распределения ключей).

В алгоритмах с асимметричным (открытым) ключом используются два ключа: один ключ – при шифровании сообщения, и другой – при расшифровке. Системы шифрования с асимметричным открытым ключом требуют больших вычислительных ресурсов по сравнению с системами с секретным симметричным ключом. Поэтому обычно шифрование с открытым ключом используют для распределения ключей (для обмена ключами) и аутентификации, т.е. для шифрования сравнительно коротких сообщений. Для шифрования больших объемов передаваемых данных используют симметричный алгоритм с секретным (закрытым) ключом [2].

Развитие вычислительной техники и появление высокоскоростных квантовых компьютеров позволит дешифровать перехваченное сообщение