Применение федеративного обучения для построения систем обнаружения вторжений

Е. С. Новикова[1] Е.В. Федорченко[2]

[1]Факультет компьютерных технологий и информатики
СПбГЭТУ "ЛЭТИ"

[2]Лаборатория проблем компьютерной безопасности
СПБ ФИЦ РАН

РусКрипто, 21 – 24 марта 2023

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

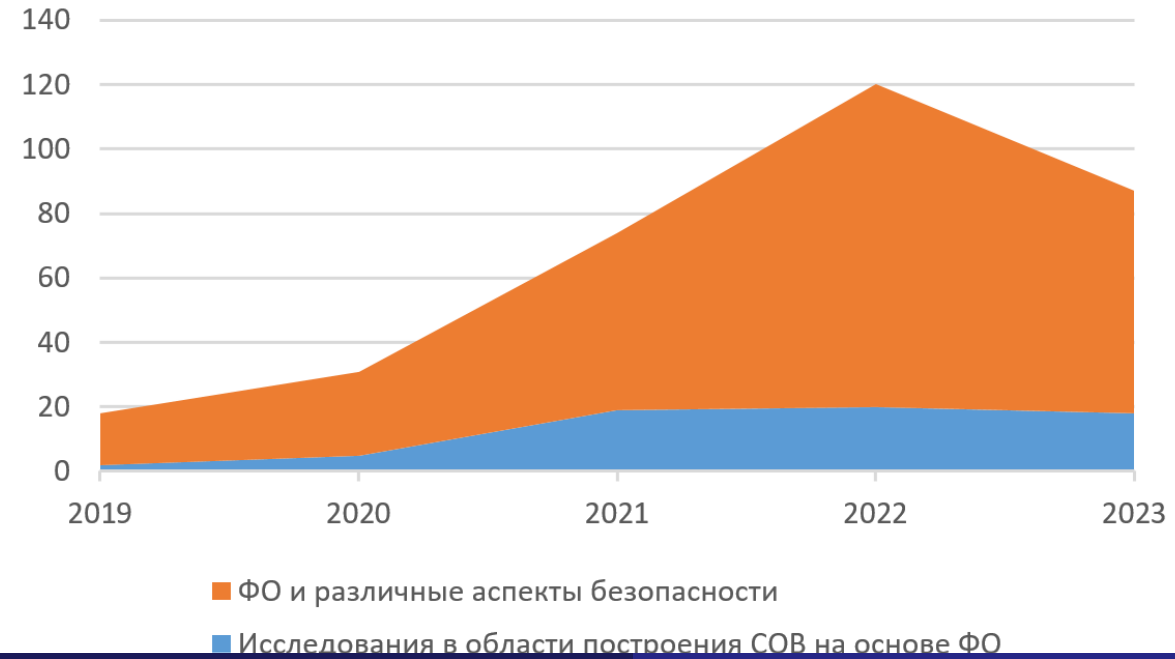
Санкт-Петербургский
Федеральный исследовательский центр
Российской академии наук

Содержание

Актуальность исследования

- В 2016 была разработана концепция федеративного обучения (ФО), позволяющая организовать распределенное машинное обучение, обеспечивающее конфиденциальность обучающих наборов данных, т.е. конфиденциальность владельцев данных
- ФО активно исследуется как способ построения адаптивных систем обнаружения вторжений (СОВ), обеспечивающих конфиденциальность анализируемых данных

Статистика публикаций, посвященных ФО



- Рецензируемые журналы и тезисы конференций
- ScienceDirect и IEEE Explore
- Ключевые слова: federated learning AND Intrusion detection

Цели исследования

Систематизация следующих аспектов применения ФО

- Архитектурные решения СОВ на основе ФО
- Схемы распределения данных
- Обучающие наборы данных: подходы к моделированию распределения данных между клиентами
- Метрики оценки эффективности разработанных решений

Федеративное обучение: основные характеристики

Основные компоненты ФО:

- клиенты, которые владеют данными и обучают локальную модель;
- сервер, который координирует весь процесс обучения и вычисляет глобальную модель;
- коммуникационно-вычислительная среда, которая обеспечивает обмен параметрами модели.

Ключевые характеристики ФО:

- схема взаимодействия между клиентами: централизованная и децентрализованная схема
- вычислительные и сетевые ресурсы сотрудничающих владельцев данных: федерация IoT устройств и федерация организаций
- схема разделения данных между клиентами: горизонтальное и вертикальное распределение данных

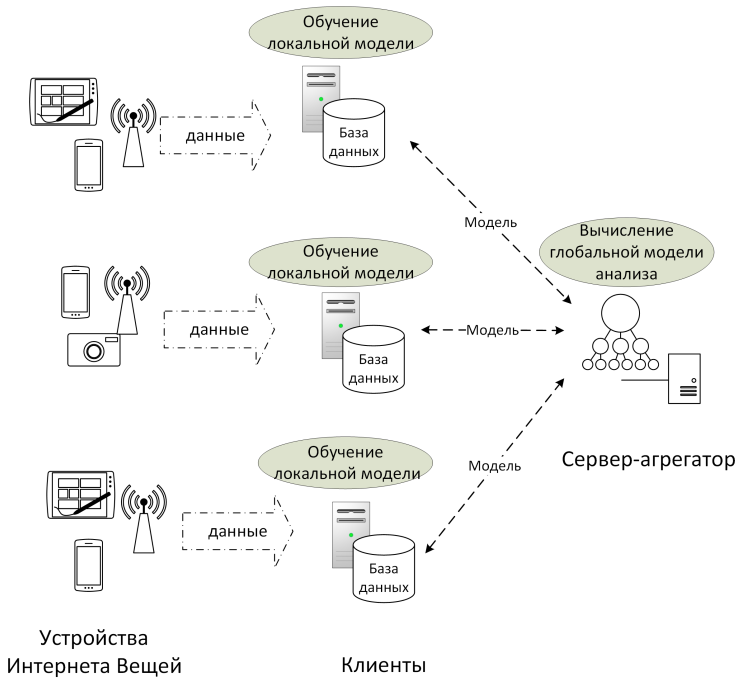
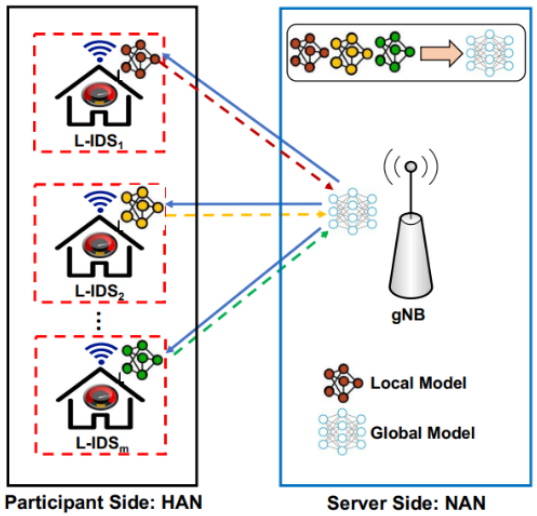


Схема взаимодействия между узлами в СОВ на основе ФО

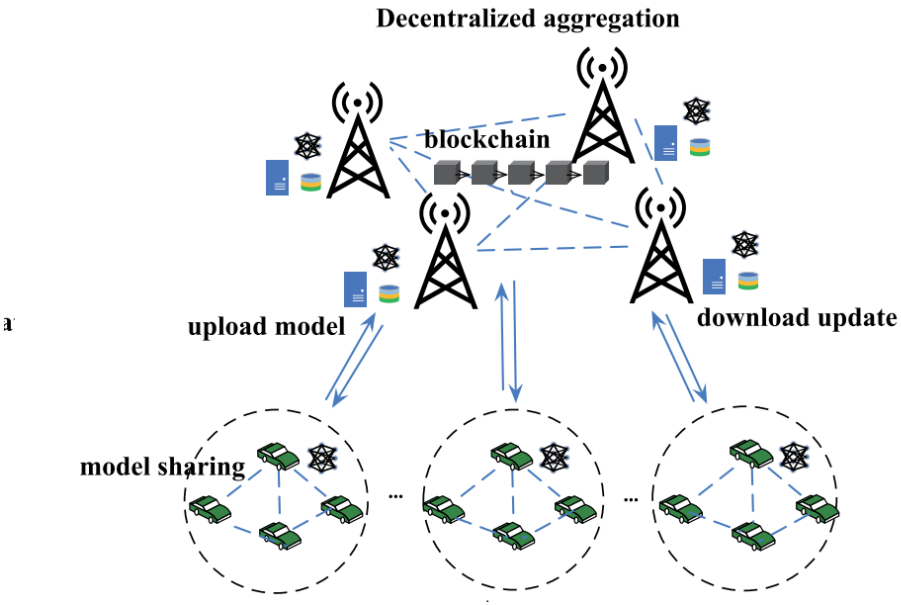
Централизованная схема взаимодействия



- сетевая безопасность
- системы на основе IoT-технологий:
  - медицинские устройства
  - промышленные системы
  - сельскохозяйственные интеллектуальные системы

P. H. Mirzaee et al.,"FIDS: A Federated Intrusion Detection System for 5G Smart Metering Network,"2021 17th International Conference on Mobility, Sensing and Networking (MSN), Exeter, UK, 2021, pp. 215-222.

Децентрализованная схема взаимодействия

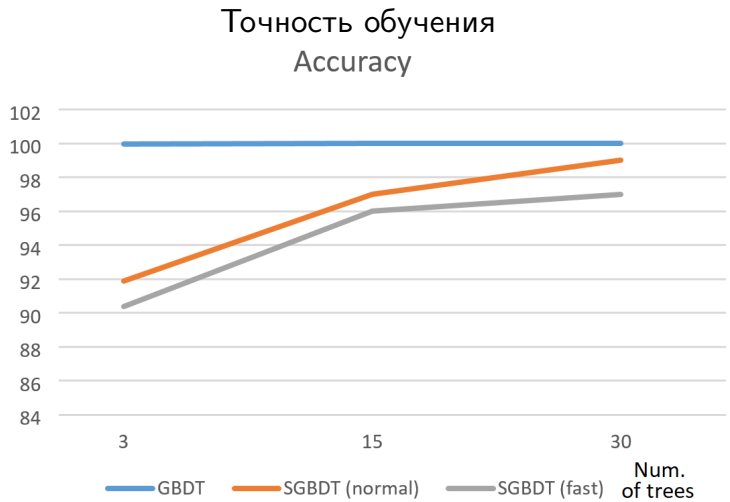


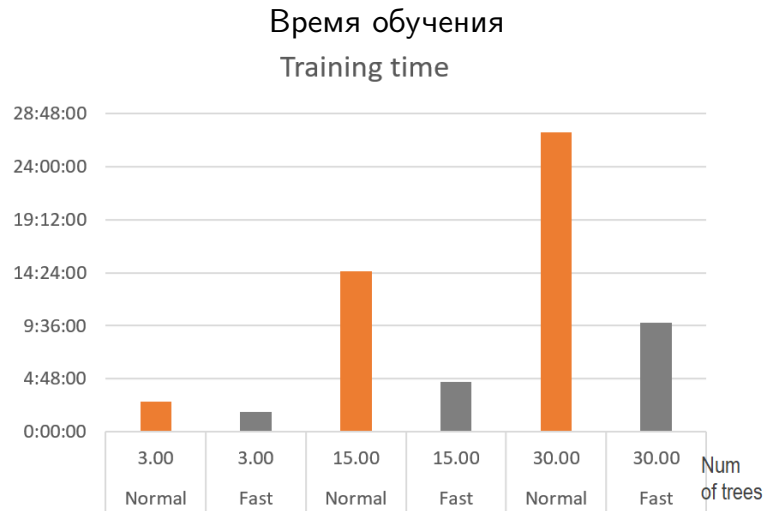
- интеллектуальные транспортные системы

H. Liu et al., "Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing,"in IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 6073-6084, June 2021, doi: 10.1109/TVT.2021.3076780.

Схемы разделения данных в СОВ на основе ФО

- Горизонтальное разделение данных - **основной сценарий использования ФО**
- Вертикальное разделение данных - 1 работа [Novikova et al., 2022]
  - Набор данных SWAT, разбиение по процессам (6 взаимодействующих клиентов)
  - Использование фреймворка FATE для организации ФО
  - Модель анализа - градиентный бустинг над деревьями решения с гомоморфным шифрованием *SecureBoost*





[Novikova et al., 2022] Novikova E., Doynikova E., Golubev S. Federated Learning for Intrusion Detection in the Critical Infrastructures: Vertically Partitioned Data Use Case // Algorithms. — 2022. — T. 15, No 4. — ISSN 1999-4893. — DOI: 10.3390/a15040104. —URL: https://www.mdpi.com/1999-4893/15/4/104.

Подходы к моделированию распределения данных между клиентами (1/2)

Подходы к моделированию распределения данных между клиентами (2/2)

Моделирование неидентично распределенных данных

- Один набор данных распределяется между разными клиентами, каждый участник получает определенный тип атак (или несколько типов атак)
- Используется несколько наборов данных, у каждого клиента один набор данных

ToN-IoT-v2

Class	Training	Validation	Testing
Benign	26500	11357	16167
Backdoor	187	80	85
DDoS	19572	8388	12040
DoS	6259	2682	3724
Injection	6726	2882	4078
MITM	58	25	41
Password	10982	4706	6869
Ransomware	33	14	18
Scanning	10508	4503	6324
XSS	23772	10188	14692
Total	104595	44827	64038

BoT-IoT-v2

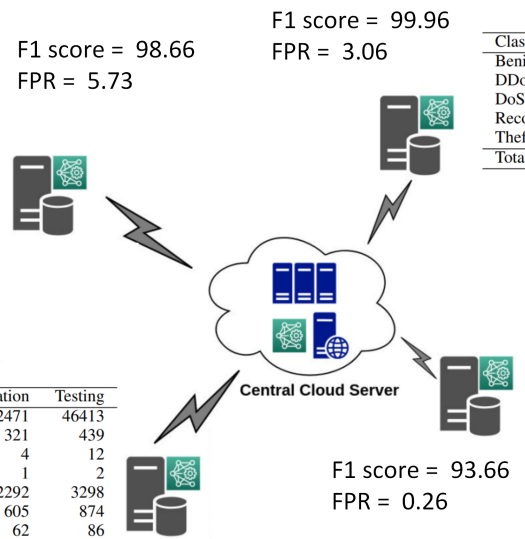
Class	Training	Validation	Testing
Benign	638	274	373
DDoS	41383	17736	25433
DoS	81876	35090	50038
Reconnaissance	12687	5437	7783
Theft	18	8	7
Total	136602	58544	83634

CIC-IDS2018-v2

Class	Training	Validation	Testing
Benign	75765	32471	46413
Bot	750	321	439
Brute Force-Web	8	4	12
Brute Force-XSS	1	1	2
DDOS attack-HOIC	5347	2292	3298
DDoS attacks-LOIC-HTTP	1412	605	874
DoS attacks-GoldenEye	144	62	86
DoS attacks-Hulk	2120	909	1332
DoS attacks-SlowHTTPTest	59	25	49
DoS attacks-Slowloris	34	14	21
FTP-BruteForce	135	58	74
Infiltration	550	236	301
SQL Injection	5	2	1
SSH-Bruteforce	467	200	240
Total	86797	37199	53142

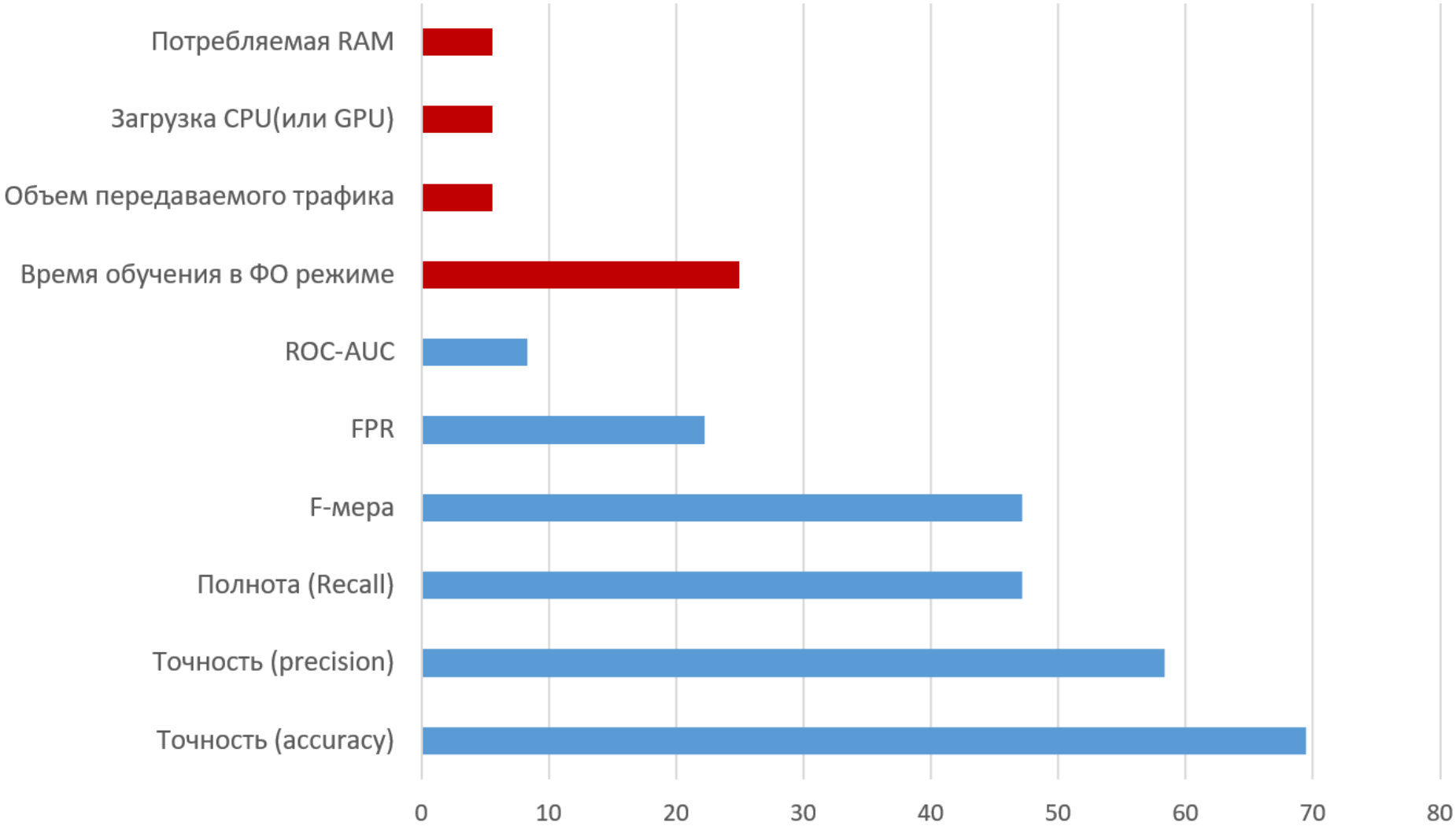
UNSW-NB15-v2

Class	Training	Validation	Testing
Analysis	36	15	20
Backdoor	32	14	19
Benign	223364	95727	136660
DoS	328	140	193
Exploits	2884	1236	1782
Fuzzers	1481	635	923
Generic	268	115	193
Reconnaissance	631	271	407
Shellcode	57	24	46
Worms	13	6	19
Total	229094	98183	140262



Popoola S. I. [и др.]. Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks // 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). — 2021. — С. 1—6. — DOI: 10 . 1109 / VTC2021 -Fall52928.2021.9625505.

Метрики оценки СОВ на основе ФО



Выводы: преимущества использования ФО для построения СОВ

- СОВ на основе ФО позволяют обрабатывать данные с ограниченным доступом, например, персональные данные и/или конфиденциальные данные.
- Методы трансферного обучения естественным образом реализуются в СОВ на основе ФО.
- Модели выявления аномалий и/или атак, обученные в федеративном режиме на нескольких наборах данных, которые содержат разные типы атак, обладают более высоким уровнем детектирования ранее неизвестных атак по сравнению с моделями, обученными на одном наборе данных.
- Возможность построения децентрализованной СОВ на основе ФО позволяет решить проблему нарушения работоспособности центрального узла, управляющего процессом обнаружения вторжения и/или аномалий, включая переобучение соответствующих моделей анализа.

Выводы: открытые вопросы

- Отсутствуют подходы, позволяющие эффективно обрабатывать вертикально распределенные данные.
- Существует необходимость в разработке методологии оценки СОВ, построенных на основе принципов ФО, которая будет определять требования к
  1. наборам данных для тестирования,
  2. моделированию различного распределения данных между взаимодейсвтвующими клиентами,
  3. метрикам, используемым для оценки эффективности аналитических моделей и пропускной способности обучения
  4. настройкам федеративного обучения (функции агрегирования, раунды агрегирования)...

Спасибо за внимание

Контактная информация:

- Е. С. Новикова: ✉ esnovikova@etu.ru
- Е. В. Федорченко: ✉ doynikova@comsec.spb.ru

SCAN ME

Исследование выполнено за счет гранта Российского научного фонда (проект № 22-21-00724)