TOWARDS FEDERATED LEARNING AT SCALE: SYSTEM DESIGN

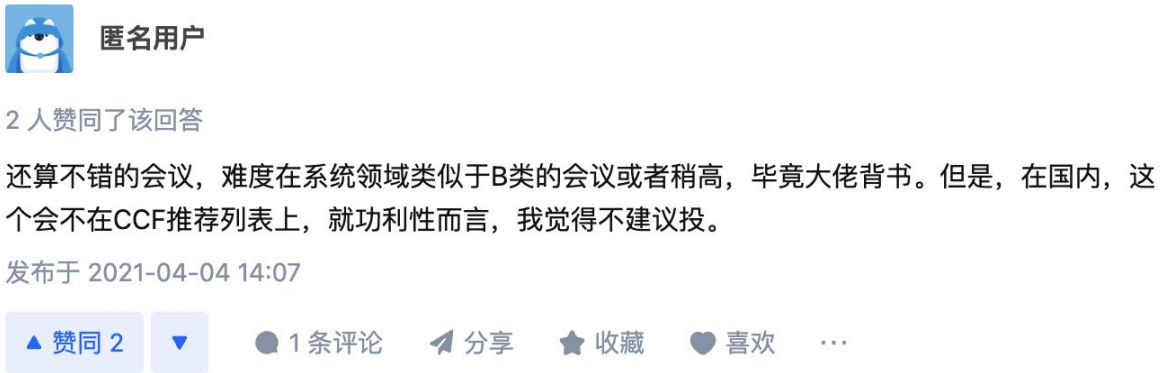
Kallista A. Bonawitz, Hubert Eichner, Wolfgang Grieskamp

Google

MLSys 2019

Background

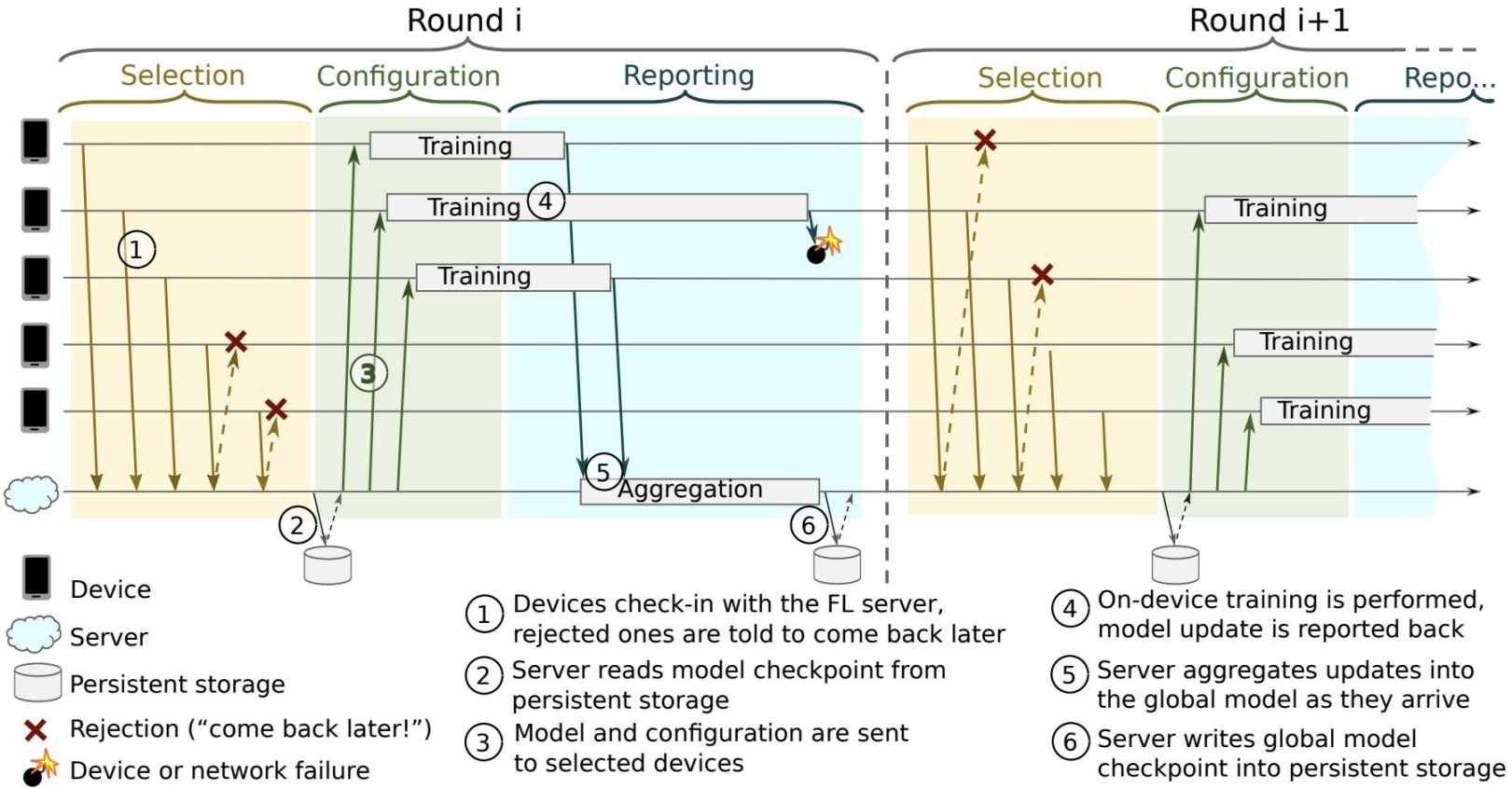
- **贡献**：提出了一种可以在工业界使用的FL框架
  - 处理设备对数据分布对复杂依赖（如时区依赖）
  - 处理不可靠的设备连接和执行中断的情况
  - 已能应对 tens of millions的设备，期待应对 billions 的设备
  - 尚处于早期版本
  - 没有开源



Components

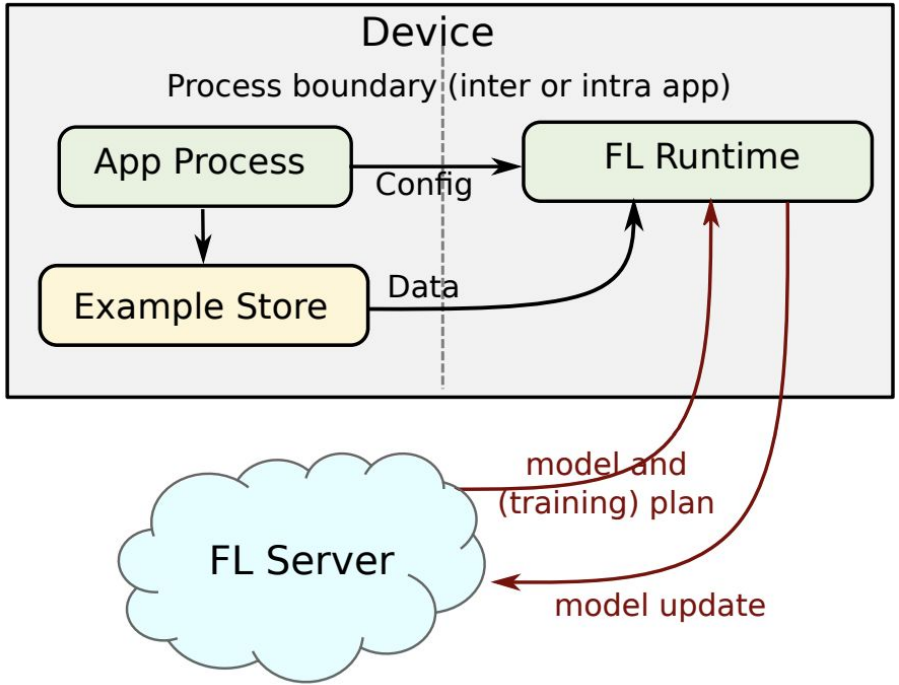
- 成员
  - 用户/devices(android手机)
  - FL server
- FL plan
  - 例如 FedAvg、secAgg
- 流程
  - 贡献者选择
  - 配置:根据FL plan
  - 报告:server收集、聚合、发放
- Pace Steering (k8s既视感)
  - 少用户:使用一个无状态的概率算法向被拒绝的设备建议重新连接的时间等
  - 多用户:随机化设备的签到时间, 避免"thundering herd"等
  - 避免在高峰期的过度活动 etc.

Phases


Round i
Round i+1
Selection
Configuration
Reporting
Selection
Configuration
Repo...
Training
Training
Training
Training
Training
Training
Aggregation
1
2
3
4
5
6
Device
Server
Persistent storage
Rejection (“come back later!”)
Device or network failure
1 Devices check-in with the FL server, rejected ones are told to come back later
2 Server reads model checkpoint from persistent storage
3 Model and configuration are sent to selected devices
4 On-device training is performed, model update is reported back
5 Server aggregates updates into the global model as they arrive
6 Server writes global model checkpoint into persistent storage

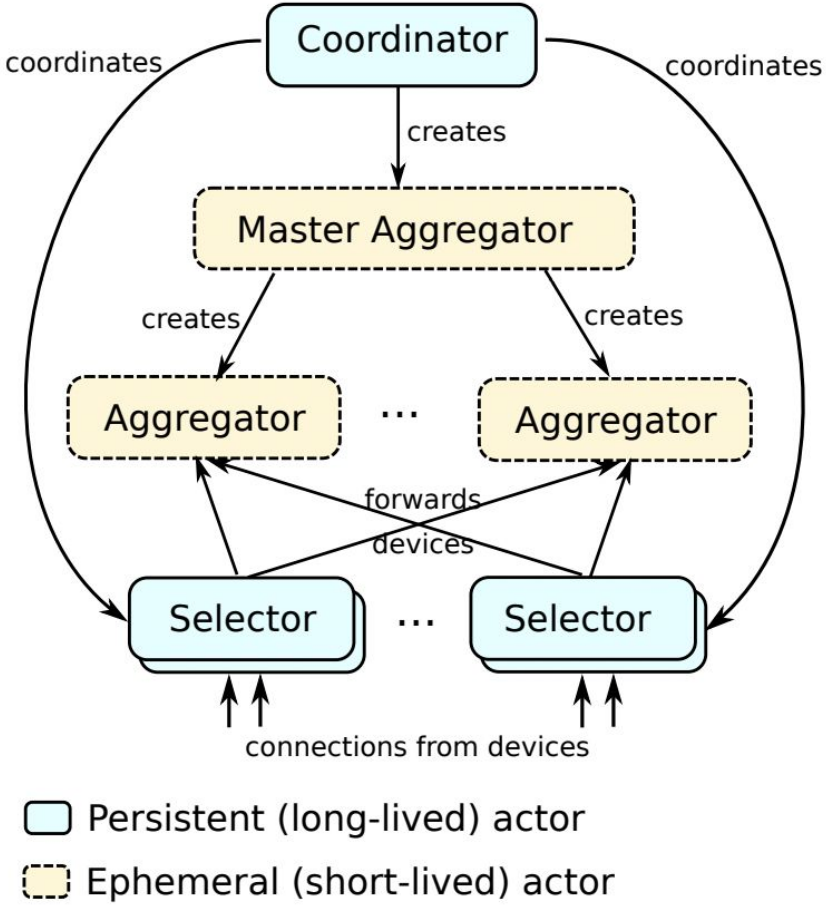
Devices

- APP通过实现提供的API，将他们的数据作为一个 样例仓库（例如一个SQLite数据库）提供给FL运行时
- 样例仓库定期清理旧数据保护数据隐私

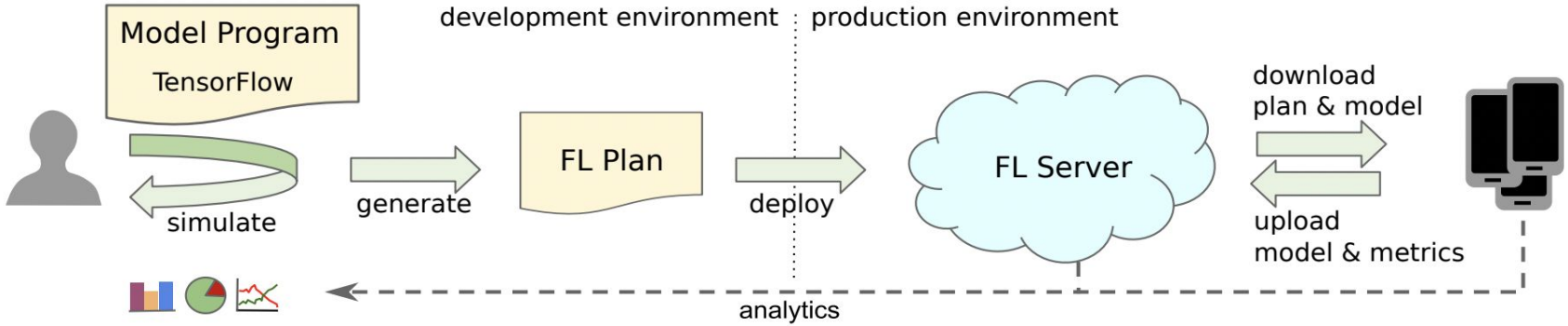


Server

- 演员模型(高并发模型)
- Master Aggregator
  - 管理epoch、update_size等
  - 根据参与方人数等，生成子 aggregator并派发任务
- 鲁棒性：
  - 一个aggregator的crash不会造成流程终止，其它actor会继续工作



Workflow



- 模型工程师测试并制定FL Plan，后发布到生产环境
- 版本控制：
  - 多设备、设备/服务器之间使用的软件（tensorflow）版本很可能不一致、没有 统一更新
  - 使用versioned FL plan 部分解决
    - 仍会偶尔碰到不兼容问题

Discuss

- Application
  - Ranking系统
  - 内容建议(键盘)
  - Next word prediction
- Future
  - 误差(用户不平等参与)
  - 收敛时间
  - 设备调度
  - 带宽
  - 联邦计算

Conclusion

- 横向联邦学习
- 工程性十足的paper
- 大公司的味很浓