

Εθνικό Μετσόβιο Πολυτεχνείο

# On-Device Federated Learning for Human Activity Recognition

ΔΗΜΗΤΡΙΟΣ ΜΑΤΣΟΥΚΑΣ  
ΑΜ : 03116738

Επιβλέπων Καθηγητής : Τσανάκας  
Παναγιώτης

---

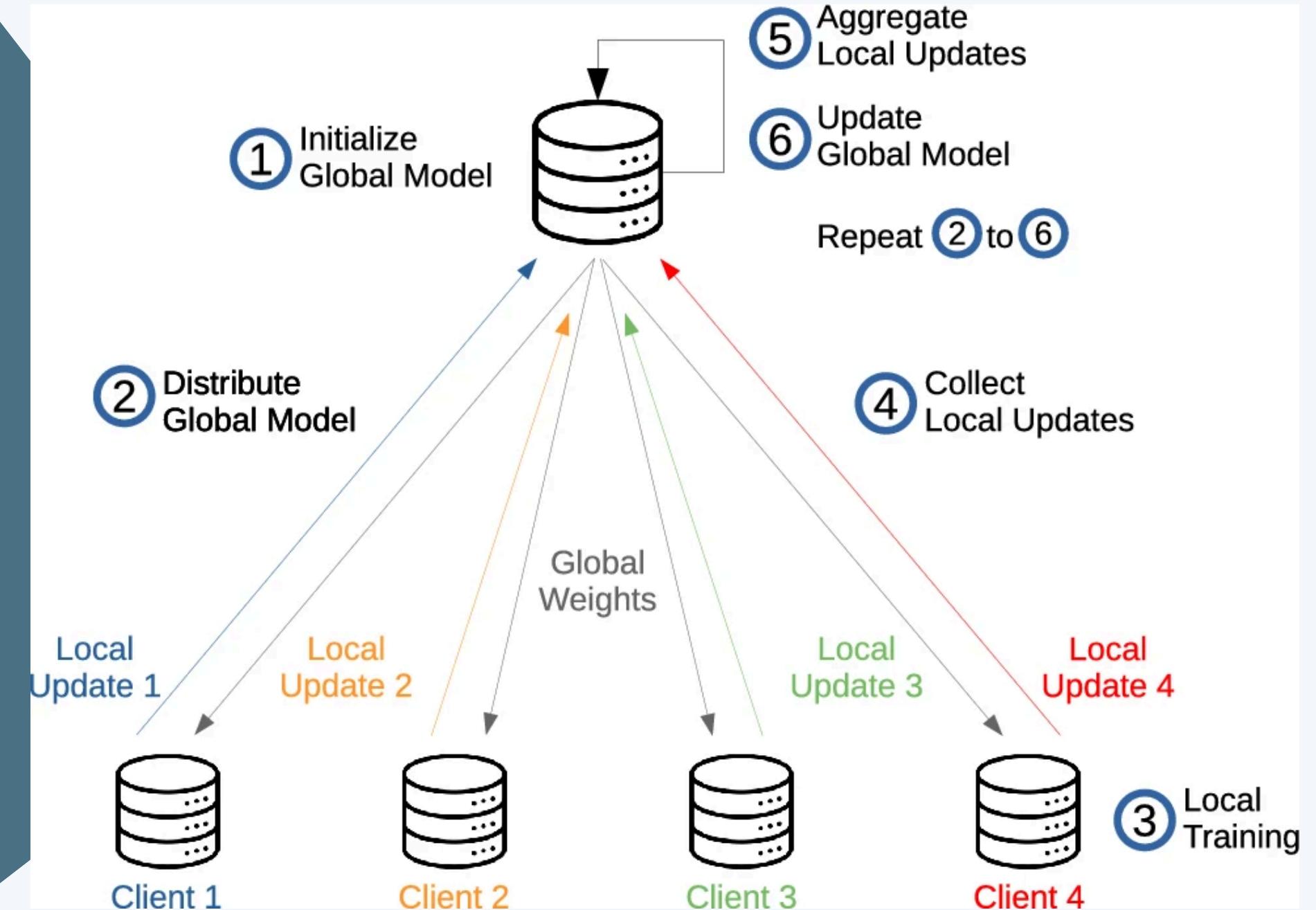
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών  
Υπολογιστών | Διπλωματική Εργασία

20 Ιουνίου 2025

# Τα Κίνητρα

Τα Smartphones και Wearables χρησιμοποιούνται από δισεκατομμύρια χρήστες και παράγουν μεγάλο όγκο δεδομένων

- Η παραδοσιακή Μηχανική Μάθηση → συγκεντρώνει δεδομένα κεντρικά (π.χ. σε προβλήματα όπως Όραση Υπολογιστών, Επεξεργασία Φυσικής Γλώσσας)
- Η Μηχανική Μάθηση αντιστοιχίζει την είσοδο με την έξοδο μέσω ενός συνόλου παραμέτρων (συνήθως ονομάζονται βάρη)
- Εκπαίδευση: Τα βάρη ενημερώνονται ώστε το μοντέλο να μαθαίνει από δεδομένα
- Πρόβλεψη (inference): Το μοντέλο χρησιμοποιεί τα εκπαιδευμένα βάρη για να κάνει προβλέψεις σε νέα, άγνωστα δεδομένα
- Δημιουργούνται σοβαρά ζητήματα απορρήτου και προστασίας προσωπικών δεδομένων
- Αυστηροί κανονισμοί όπως GDPR και HIPAA καθιστούν αυτό το ζήτημα ιδιαίτερα κρίσιμο
- Προκύπτει ανάγκη για εκμάθηση με σεβασμό στην ιδιωτικότητα, απευθείας πάνω στη συσκευή



# Τι είναι η Ομοσπονδιακή Μάθηση (Federated Learning);

- Η εκπαίδευση γίνεται τοπικά σε κάθε συσκευή → στέλνονται μόνο ενημερώσεις μοντέλου
- Ο κεντρικός server συγκεντρώνει τις ενημερώσεις (π.χ. FedAvg)
- Δεν αποστέλλονται τα αρχικά δεδομένα – διατηρείται η ιδιωτικότητα

**Δύο βασικές διαμορφώσεις ;**

cross-device (π.χ. smartphones) & cross-silo (π.χ. νοσοκομεία)

## Προκλήσεις

Ετερογένεια δεδομένων (data heterogeneity),  
Ετερογένεια του Συστήματος (OS,  
επεξεργαστές, συνδεσιμότητα Wi-Fi/5G κ.ά.)

Τι λείπει από την υπάρχουσα  
έρευνα στην FL;



## Προσομοιώσεις

Οι περισσότερες μελέτες βασίζονται σε προσομοιώσεις με  
απλά datasets (π.χ. CIFAR-10)

## Αγνοούνται

Περιορισμοί υλικού (hardware limitations)  
Κατανάλωση ενέργειας  
Αστάθεια δικτύου

## Κενό στην έρευνα

έλλειψη υλοποιήσεων σε πραγματικές συσκευές

# Τι επιδιώκει αυτή η εργασία

- Ανάπτυξη και υλοποίηση συστήματος FL σε πραγματικά Android smartphones
- Εφαρμογή στο πρόβλημα Αναγνώρισης Ανθρώπινης Δραστηριότητας (HAR)
- Το HAR είναι ιδανική εφαρμογή:
  - Συνδυάζει ευαίσθητα προσωπικά δεδομένα
  - Έχει πρακτική αξία
  - Μπορεί να υλοποιηθεί σε υπάρχουσες συσκευές με αισθητήρες



## Η εργασία αξιολογεί

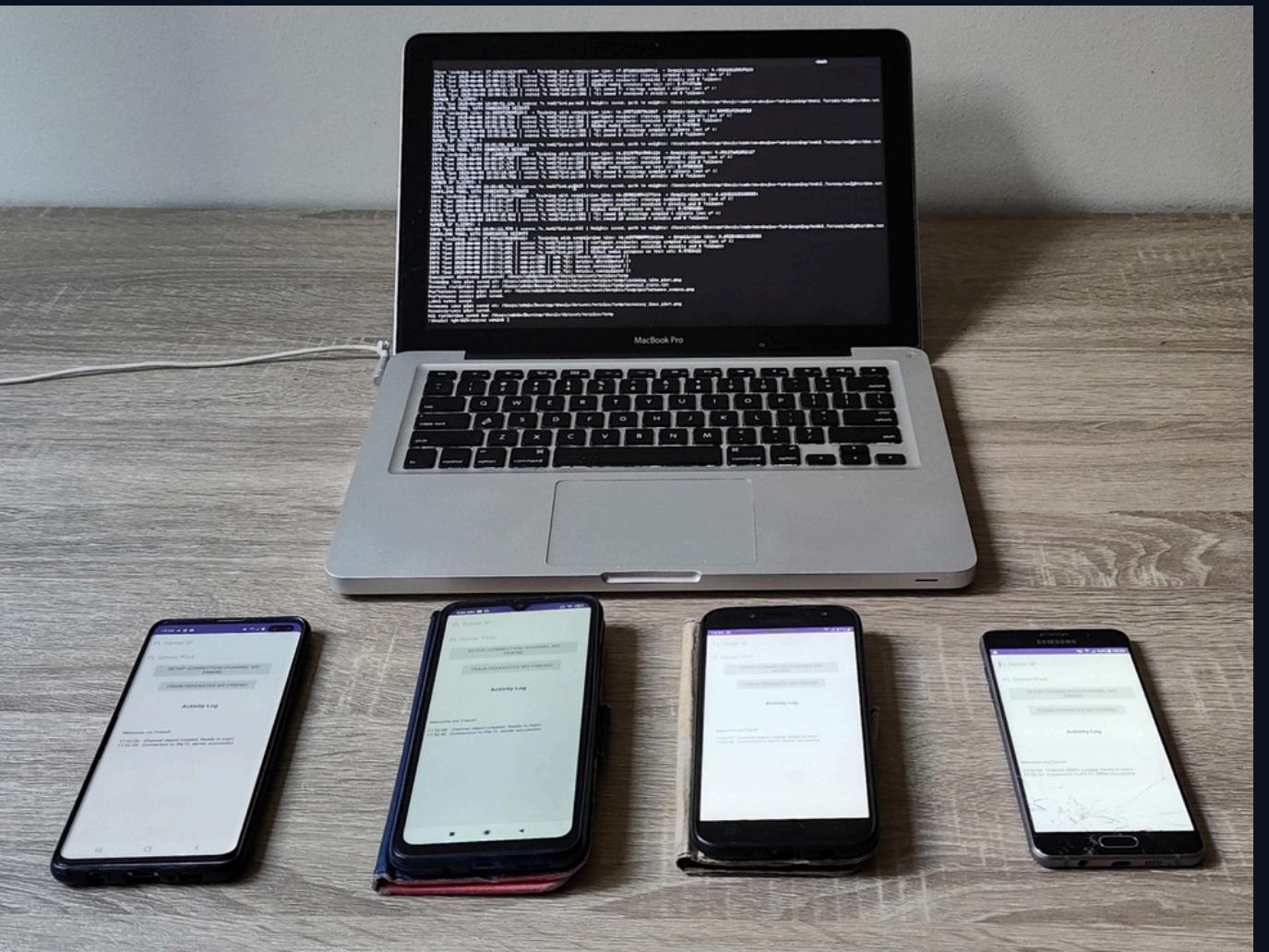
- Ετερογένεια δεδομένων
- Ενεργειακό Αποτύπωμα
- Ανθεκτικότητα σε ασταθή δίκτυα

# Αρχιτεκτονική Federated Learning Συστήματος

## Κύρια Σημεία

---

- Κεντρικός server σε laptop (Python + Flower)
- 5 Android smartphones ως clients
- Εκπαίδευση γίνεται τοπικά μέσω TensorFlow Lite (TFLite)
- Χρήση τοπικού Wi-Fi για ανταλλαγή μοντέλων



# Σχόλια για τις συσκευές μας

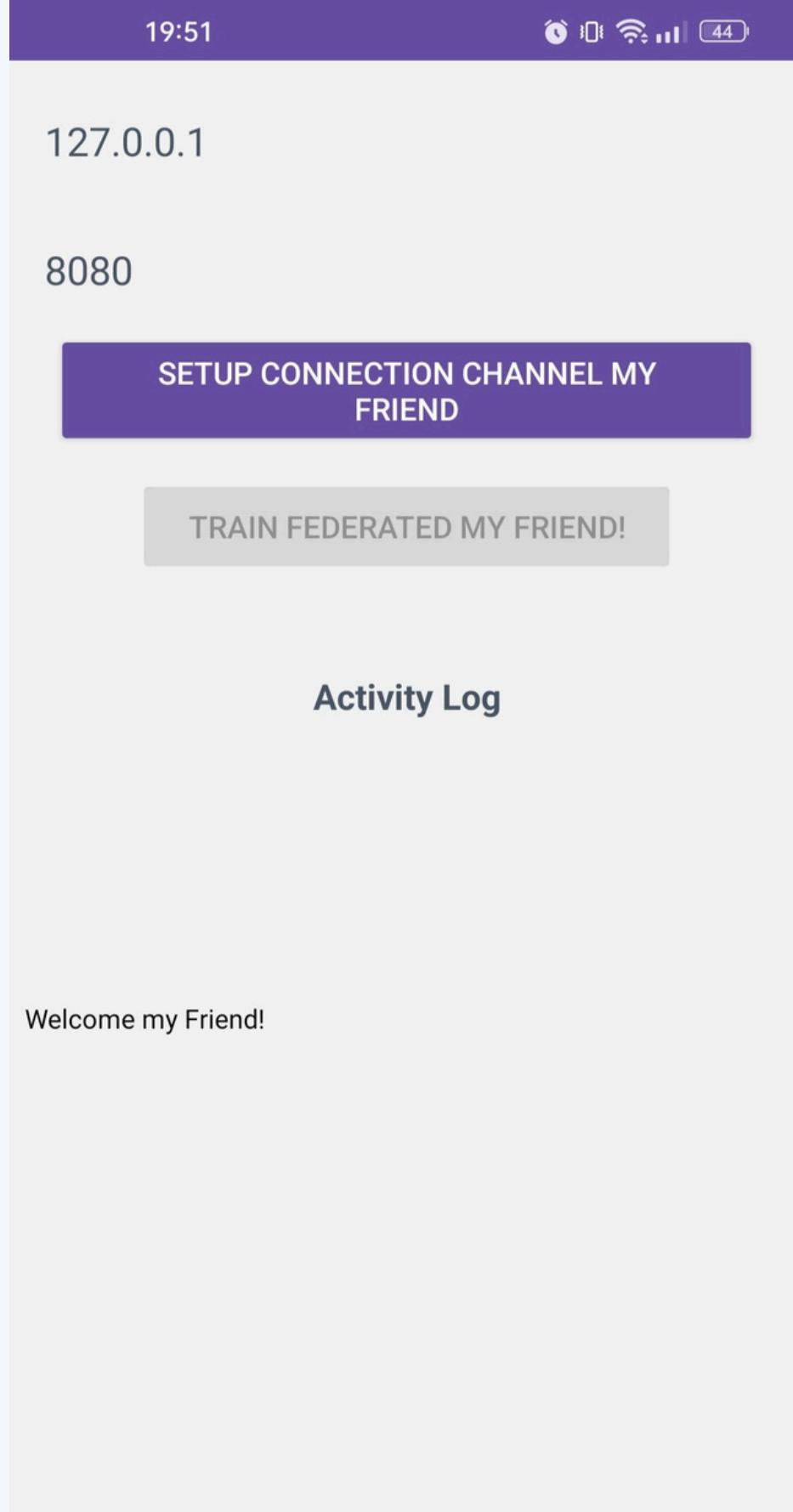
Σημαντική ετερογένεια σε υπολογιστική ισχύ και RAM

Διαφορετικές εκδόσεις Android → συστημική ετερογένεια

Συνθήκες που αντικατοπτρίζουν ρεαλιστικά περιβάλλοντα cross-device FL

Συσκευή	Έτος Κυκλοφορίας	Επεξεργαστής	RAM	Android
<b>Realme GT Neo 2 (RMX3370)</b>	2021	Snapdragon 870	8 GB	12
<b>Samsung Galaxy A5 (SM-A510F)</b>	2016	Snapdragon 615	2 GB	7
<b>Samsung Galaxy J7 (SM-J730F)</b>	2017	Exynos 7870	3 GB	8
<b>Samsung Galaxy S10+ (SM-G975F)</b>	2019	Snapdragon 855	6 GB	12
<b>Xiaomi Redmi 9C (M2006C3MNG)</b>	2020	Helio G35	2 GB	10





# Ανάπτυξη Android Εφαρμογής

- Android app σε Java, βασισμένη στο Flower Android example
- Εγκατάσταση & Εκκίνηση μέσω απλού UI (σύνδεση → "Train")
- Χρήση TFLite για on-device training
- Περιορισμός: Δεν υποστηρίζεται απευθείας ενημέρωση βαρών → αποστολή ολόκληρου μοντέλου κάθε φορά

**Χαρακτηριστικά**

# Διαδικασία του Federated Learning Κύκλου & Μετρήσεις Συστήματος



## O server Ρυθμίζει:

- Πλήθος τοπικών εποχών (local epochs)
- Πλήθος γύρων FL
- Αριθμό clients ανά γύρο
- αρχιτεκτονική του DNN μοντέλου (αριθμος και μεγεθος των hidden layers)



## Αυτοματοποιημένη Συλλογή & Απεικόνιση Μετρήσεων

- Accuracy ανά γύρο, Confusion matrix και ανά κλάση metrics (precision, recall, F1)
- Χρόνος εκπαίδευσης ανά γύρο & συνολικά
- Κατανάλωση ενέργειας (battery drop & voltage drop) ανά συσκευή και γύρο
- Αξιοπιστία δικτύου: RSSI, latency, DL/UL Speed, αριθμός ενεργών clients

# Σύνολα Δεδομένων

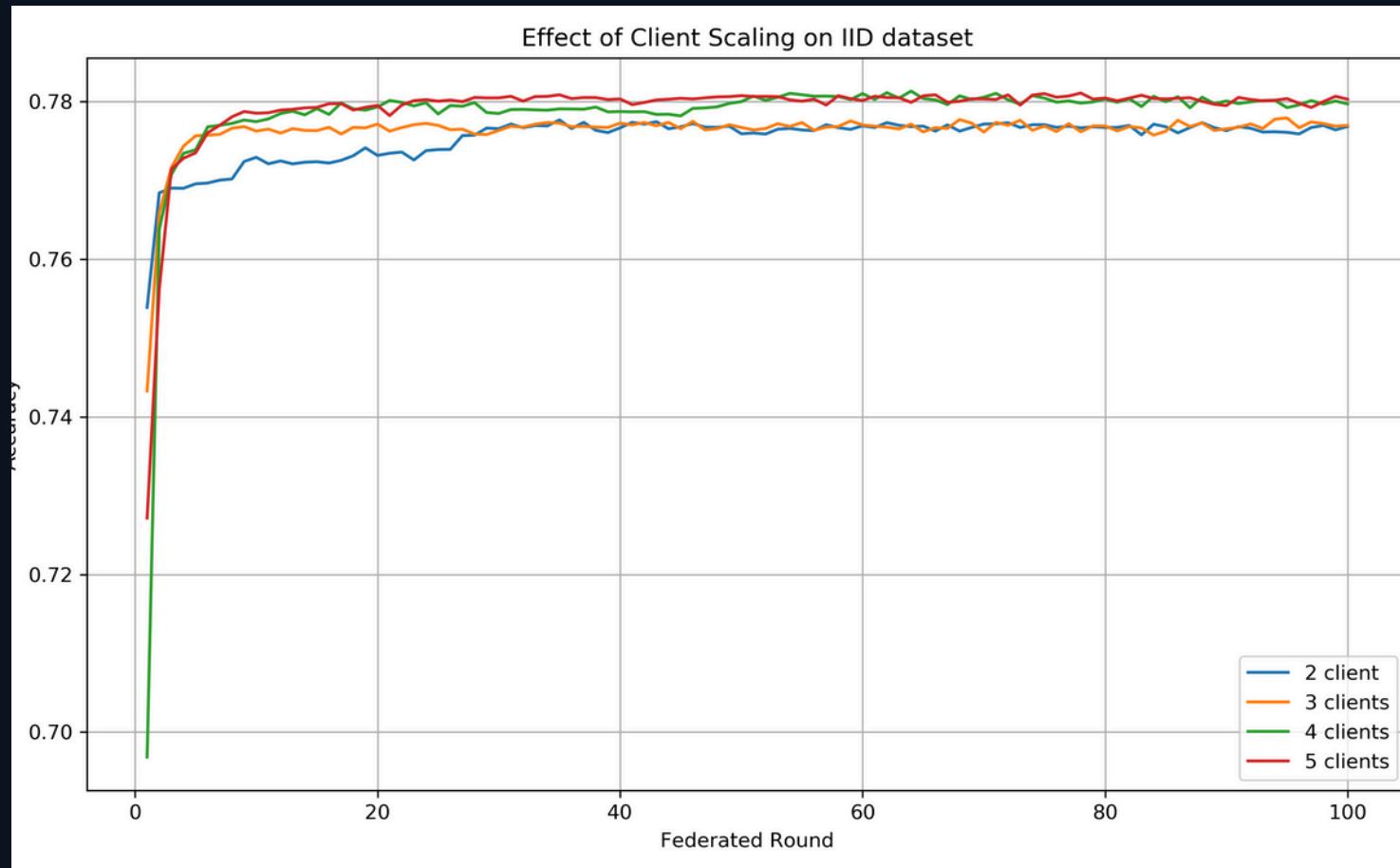
Χρήση 6 HAR datasets με διαφορετικά επίπεδα επεξεργασίας

Εργαλεία:

- **split\_to\_client()**: ανάθεση δεδομένων σε **clients**
- **class\_imbalance()**: εισαγωγή ασυμμετρίας των κλάσεων ανά **client**
- **volume\_knob()**: μεταβολή όγκου δεδομένων ανά **client**

Dataset	Δραστηριότητες (πλήθος)	Αισθητήρες	Συχνότητα Δειγματοληψίας	Υποκείμενα(subjects)	Σχολια
HARSense	6	Acc + Gyro	Άγνωστη	12	Από smartphones σε μέση & τσέπες
UCI HAR (Smartphones)	6	Acc + Gyro (Samsung Galaxy SII)	50 Hz	30	561 features, επεξεργασμένα
PAMAP2	12	IMUs + HR monitor (ECG)	100 Hz (IMU), 9 Hz (HR)	9	Κατάλληλο για ιατρικές εφαρμογές
MotionSense	6	Acc + Gyro (iPhone 6s)	50 Hz	24	raw data
MHealth	12	Acc, Gyro, Mag + ECG (πολλαπλά σημεία)	50 Hz	10	Κατάλληλο για ιατρικές εφαρμογές
PhysioNet (Acceleration)	6	Acc (Actigraph GT3X+)	100 Hz	20	αιγαϊως σηματα επιτάχυνσης

# Κλιμάκωση συσκευών: IID vs non-IID



IID: Περισσότεροι clients → το μοντέλο βλέπει περισσότερα δεδομένα → ταχύτερη σύγκλιση & υψηλότερη απόδοση

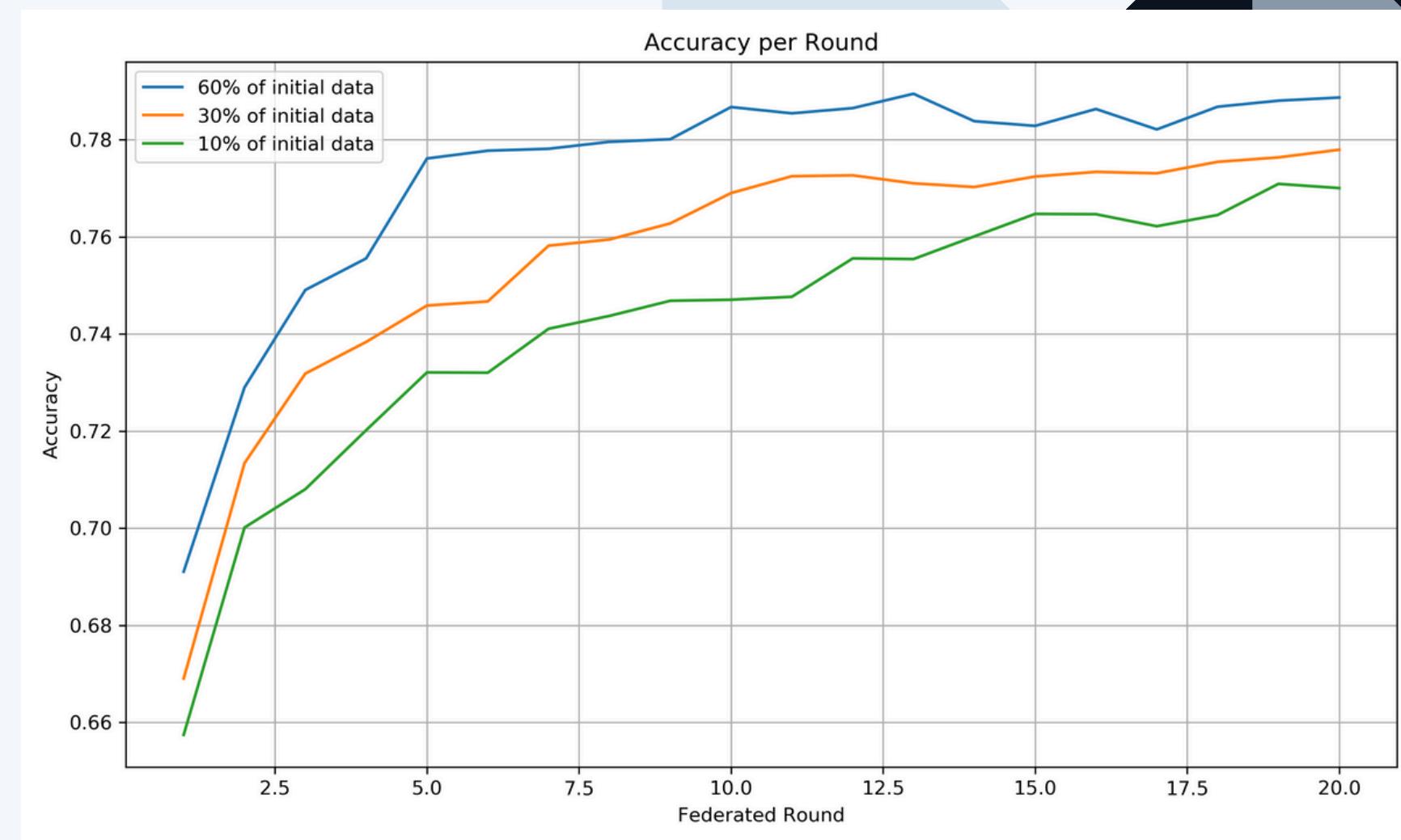
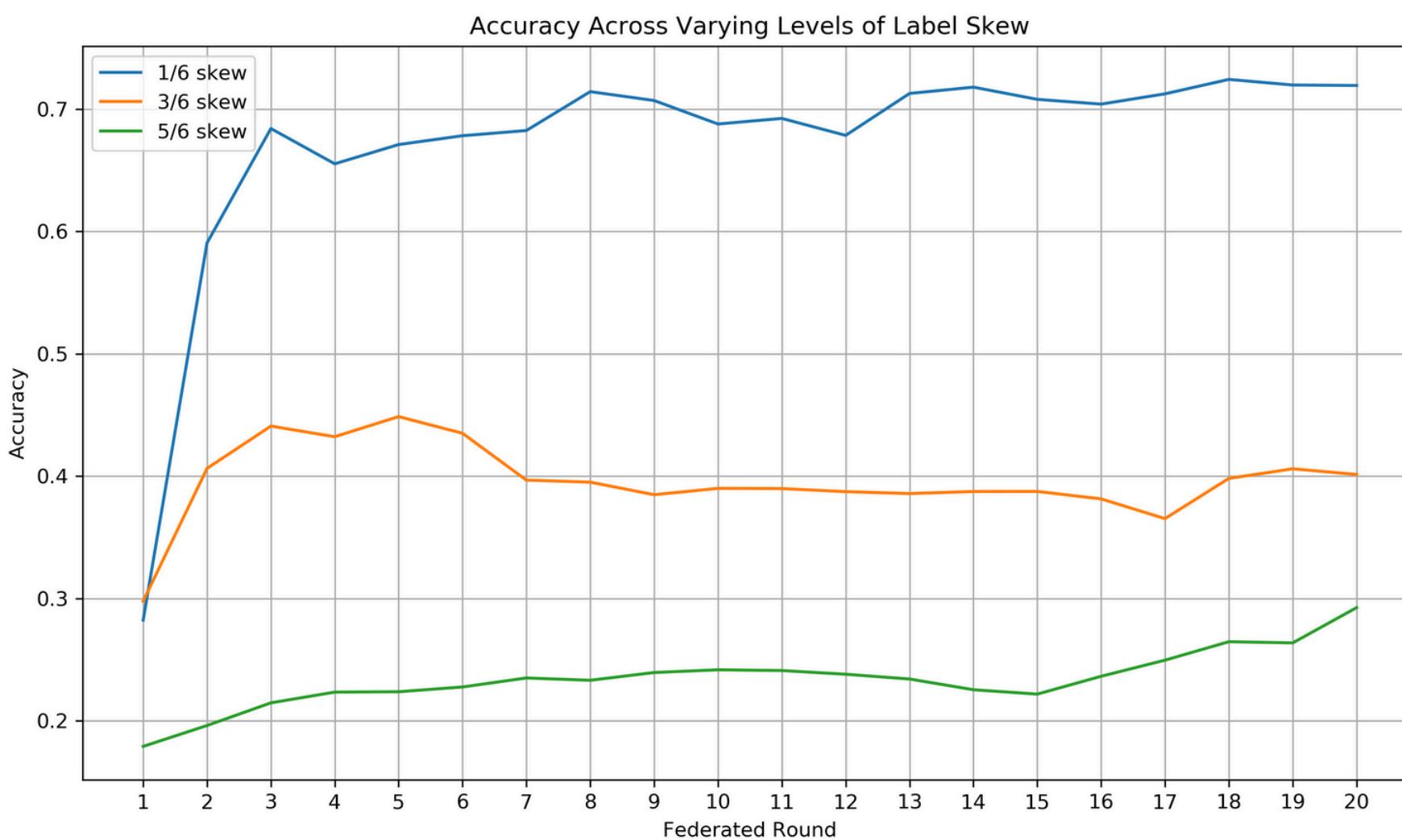


non-IID: Αν και η αύξηση των clients βελτιώνει την απόδοση, η εκπαίδευση είναι πολύ πιο δύσκολη και ασταθής

- Βλέπουμε στην non-IID ότι με 5 clients έχουμε καλύτερη σύγκλιση σε σχέση με 2 ή 3, αλλά συνολικά:
  - Η καμπύλη είναι θορυβώδης
  - Η τελική απόδοση είναι πολύ χαμηλότερη από την αντίστοιχη IID
- Αυτό το πείραμα δείχνει ότι, παρότι το scaling βοηθάει, το non-IID αποτελεί τελείως διαφορετική πρόκληση. Το μοντέλο δυσκολεύεται να γενικεύσει, καθώς κάθε client έχει πολύ "τοπική" εικόνα του προβλήματος

# Επίδραση Κατανομής Δεδομένων στην Απόδοση

- Τα πειράματα έγιναν με το HARSense dataset, το οποίο περιλαμβάνει 6 κατηγορίες δραστηριοτήτων
- Πειράματα με συμμετρία στις κλάσεις (Label Skew): Κάθε client στερείται 1, 3 ή 5 από τις 6 κλάσεις → Το μοντέλο δυσκολεύεται να γενικεύσει → πτώση ακρίβειας έως 55%
- Πειράματα με ανισοκατανομή όγκου δεδομένων (Quantity Skew): Κάθε client λαμβάνει 10%, 30% ή 60% των αρχικών δεδομένων → Μικρή επίδραση στην ακρίβεια (~2%)

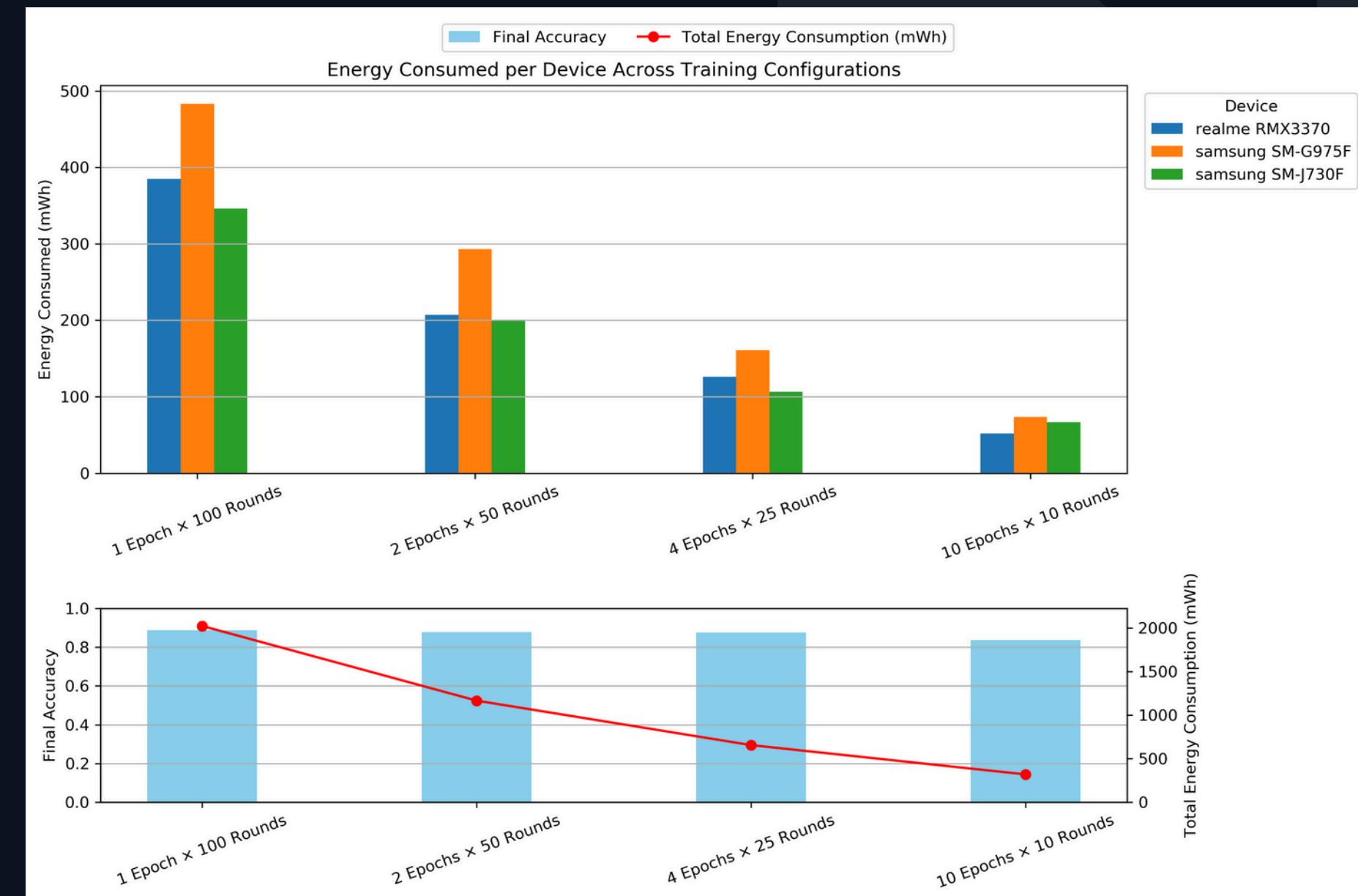


Συμπέρασμα: Η ποικιλία κλάσεων παίζει πολύ κρισιμότερο ρόλο από τον όγκο δεδομένων ανά client

# Κατανάλωση Ενέργειας

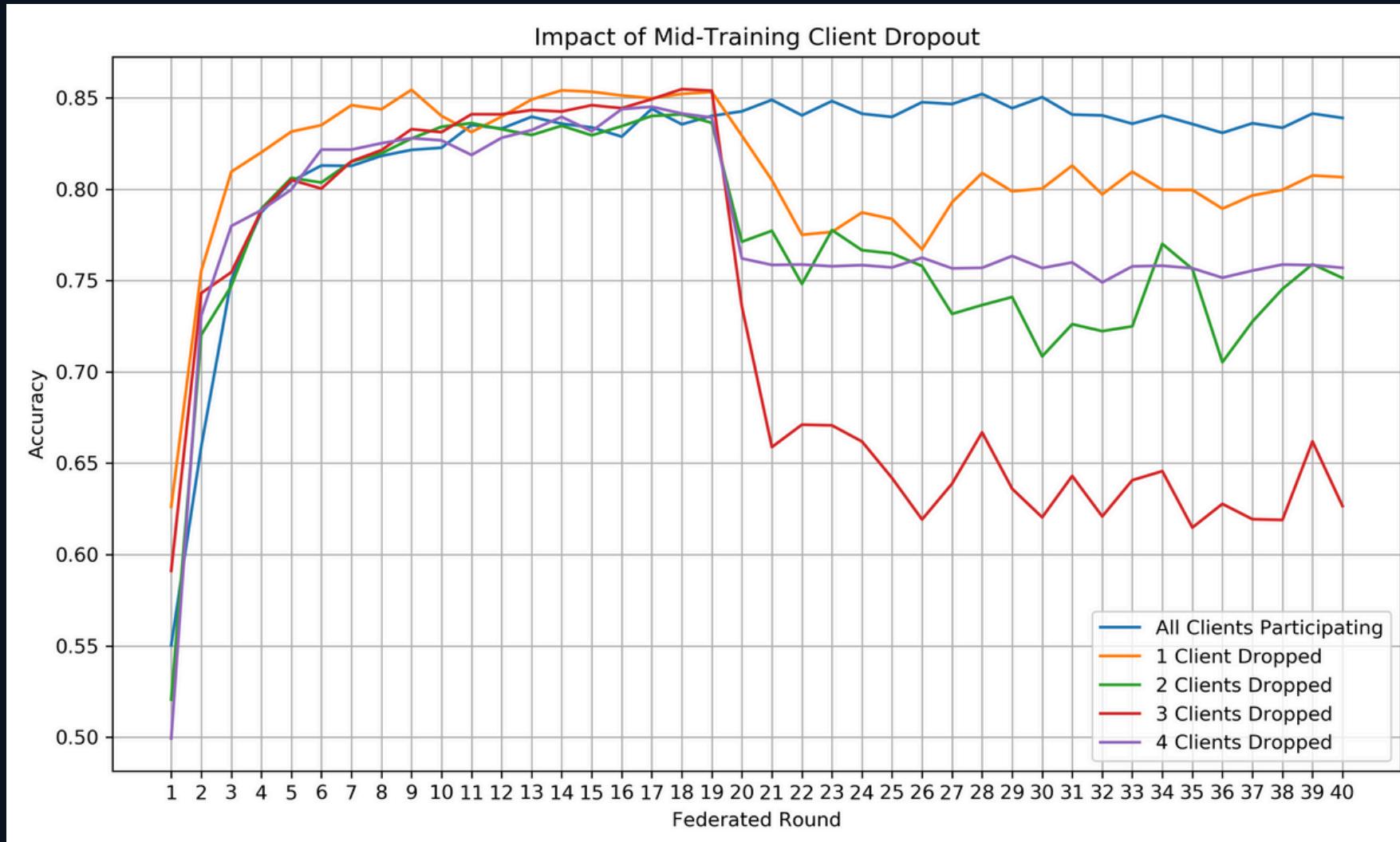
## Κύρια Σημεία

- Πειράματα με σταθερό αριθμό βημάτων SGD = 100, αλλά διαφορετικές ρυθμίσεις:  
 $1 \times 100, 2 \times 50, 4 \times 25, 10 \times 10$  (Epochs × Federated Rounds)
- Μείωση γύρων → σημαντική μείωση ενέργειας:  
Από 2023.99 mWh → 319.37 mWh  
Δηλαδή πάνω από 84% εξοικονόμηση
- Η ακρίβεια παραμένει σταθερή (μικρή διαφορά ανάμεσα σε  $1 \times 100$  και  $10 \times 10$ )
- Λιγότερες επικοινωνίες → λιγότερη ενέργεια λόγω λιγότερων network transmissions
- Οι νεότερες συσκευές (π.χ. Realme RMX3370) είναι πολύ πιο αποδοτικές ενεργειακά από τις παλαιότερες
- Το πείραμα δείχνει ότι η εξισορρόπηση τοπικής εκπαίδευσης και συγχρονισμού είναι κρίσιμη για την ενεργειακή απόδοση στο FL



# Ανθεκτικότητα σε Απώλεια Συσκευών

- Το πείραμα πραγματοποιήθηκε με το HARSense dataset σε συνθήκη label skew 3/6 (κάθε client είχε μόνο 3 από τις 6 ετικέτες)
- Το πείραμα ξεκινά με 5 ενεργούς clients που συμμετέχουν σταθερά στους γύρους 1–20
- Στο γύρο 21, γίνεται τεχνητό dropout:
  - 1 έως 4 clients αποχωρούν, ανά σενάριο
- Η ακρίβεια πέφτει άμεσα και αισθητά καθώς αυξάνονται τα dropouts:
  - Με 3 clients εκτός, η ακρίβεια υποχωρεί έως και 25%
  - Με 4 clients εκτός, το μοντέλο αδυνατεί να διατηρήσει σταθερή απόδοση
- Το βασικό aggregation (FedAvg) δεν προσαρμόζεται στις απώλειες → χρειάζονται robust στρατηγικές όπως:
  - FedProx, SCAFFOLD ή adaptive client selection



**Συμπέρασμα: η σταθερότητα συμμετοχής clients είναι κρίσιμη, ειδικά σε real-world FL σενάρια**

# Συμπεράσματα & Επόμενα Βήματα

## Συμπεράσματα

- Η κλίμακα συμμετεχόντων clients βελτιώνει την απόδοση σε όλα τα σενάρια (IID & non-IID). Ωστόσο στην non-IID περίπτωση η εκπαίδευση είναι πολύ πιο δύσκολη και ασταθής
- Label skew είναι ο σημαντικότερος παράγοντας που επηρεάζει την ακρίβεια του παγκόσμιου μοντέλου
- Ο αριθμός των federated γύρων είναι ο βασικός μοχλός κατανάλωσης ενέργειας
- Dropouts έχουν έντονο αρνητικό αντίκτυπο στη σύγκλιση ακόμα και όταν βρίσκονται στην μέση της εκπαίδευσης

## Επόμενα Βήματα

- Ενσωμάτωση robust aggregation μεθόδων (FedProx, SCAFFOLD) για βελτίωση σε non-IID δεδομένα
- Επέκταση σε περισσότερους clients, πιο σύνθετα μοντέλα (CNN, RNN) και άλλα προβλήματα (οπως τα Network Intrusion Detection Systems).
- Ενσωμάτωση τεχνικών προστασίας ιδιωτικότητας όπως Differential Privacy ή Secure Aggregation



**Thank You**  
For Your Attention

Δημήτριος Ματσούκας  
Ιούνιος | 2025