

HUST

ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

ONE LOVE. ONE FUTURE.



ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Khảo sát các phương pháp FL cho dữ liệu Non-IID trong bài toán ETC

ONE LOVE. ONE FUTURE.

Mục tiêu khảo sát

Tìm các phương pháp SOTA (2022–2025) xử lý non-IID và phù hợp với bài toán Encrypted Traffic Classification trong môi trường SDN đa miền.



Các hướng tiếp cận

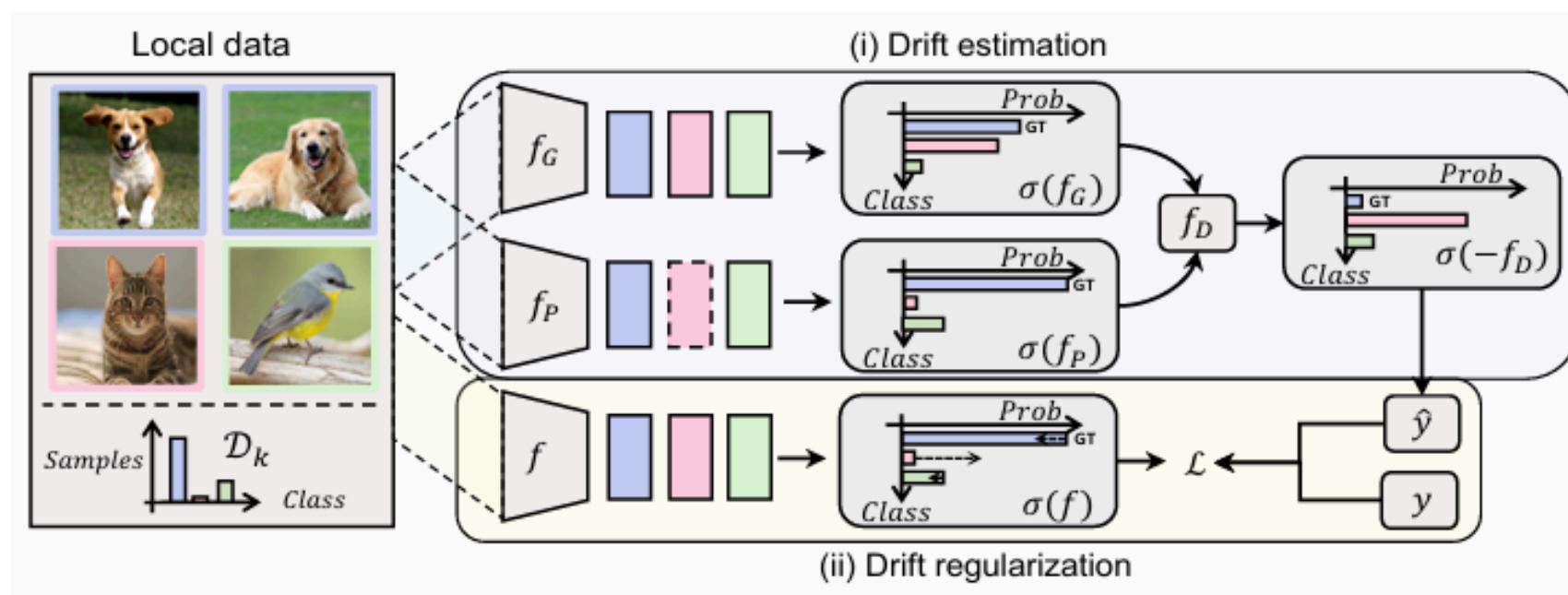
- Regularization / Proximal (FedProx, DriftReg).
- Variance reduction & control variates (SCAFFOLD).
- Representation / Contrastive (MOON, FedCoSR, FedPCL).
- Personalization & clustering (Ditto, FedALA, Adaptive Clustering).
- Hybrid (distillation, prototype, server learning).



Drift Regularization (2023)

- Thêm penalty term trong loss để hạn chế sự drift giữa local và global models. Regularizer giúp giới hạn cập nhật cục bộ.
- Ưu điểm: Ổn định cập nhật; giảm divergence; giữ cân bằng local vs global.

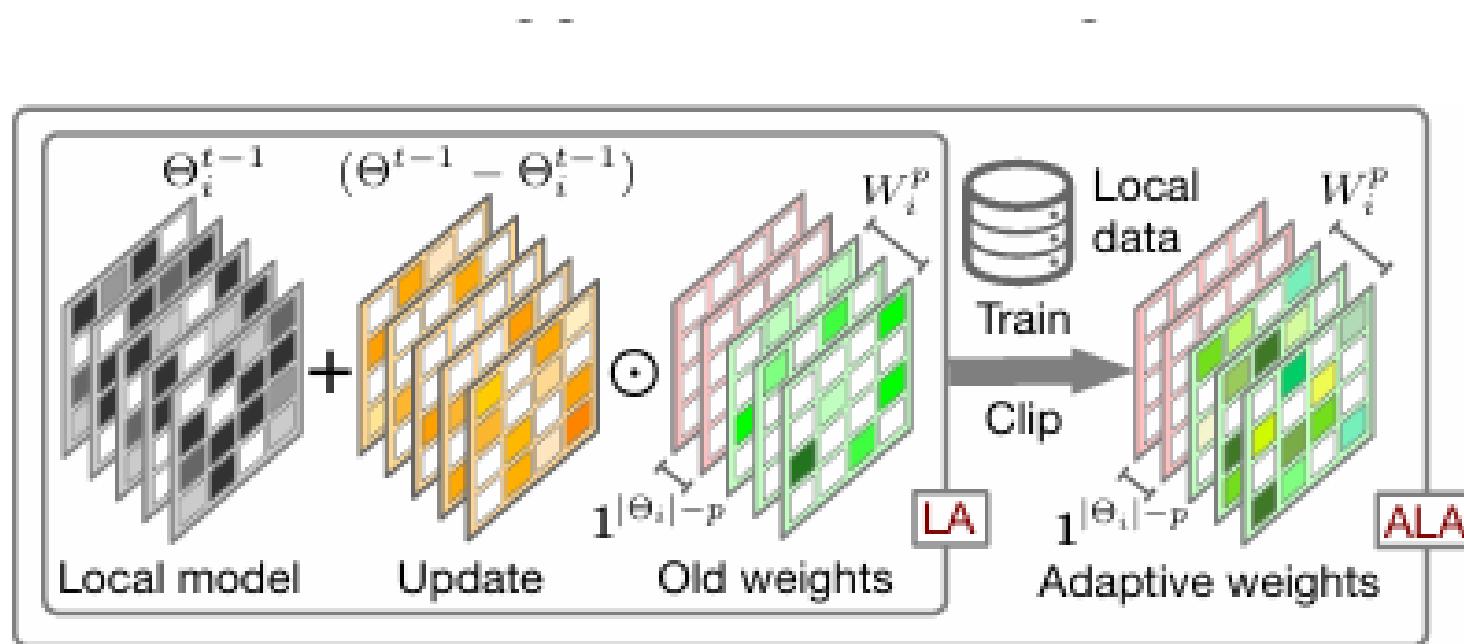
<https://arxiv.org/abs/2309.07189>



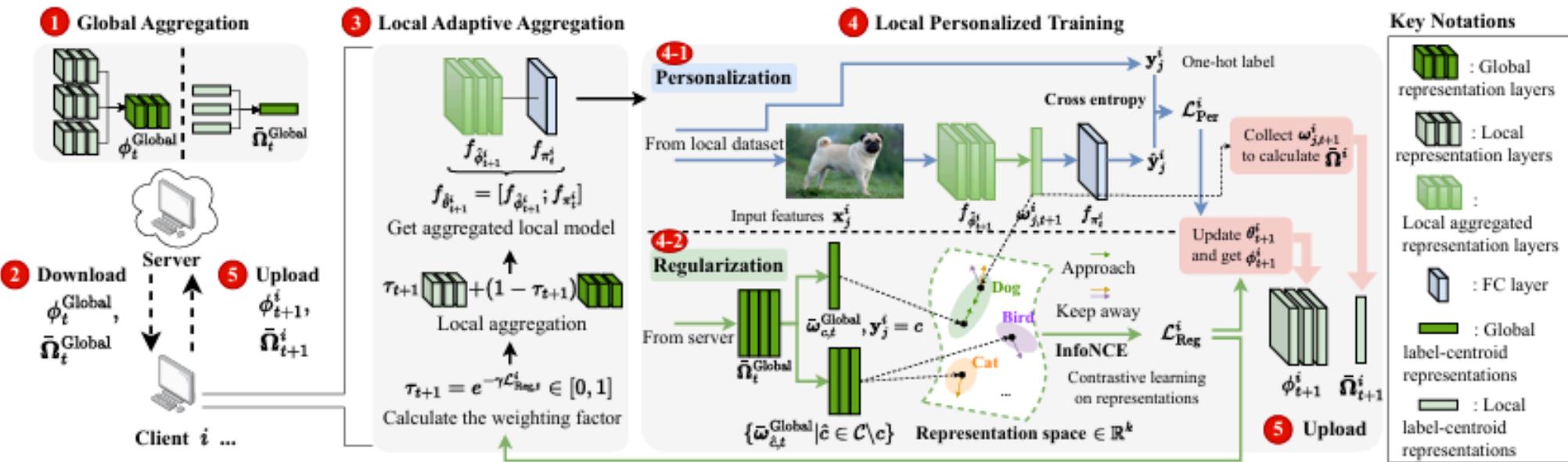
FedALA (2022)

- Mỗi client có trọng số riêng, cập nhật adaptive dựa trên alignment gradient. Tính tương quan gradient giữa client và global để điều chỉnh trọng số khi aggregate.
- Ưu điểm: Giảm negative transfer; dễ triển khai; cải thiện local accuracy.

<https://arxiv.org/abs/2212.01197>



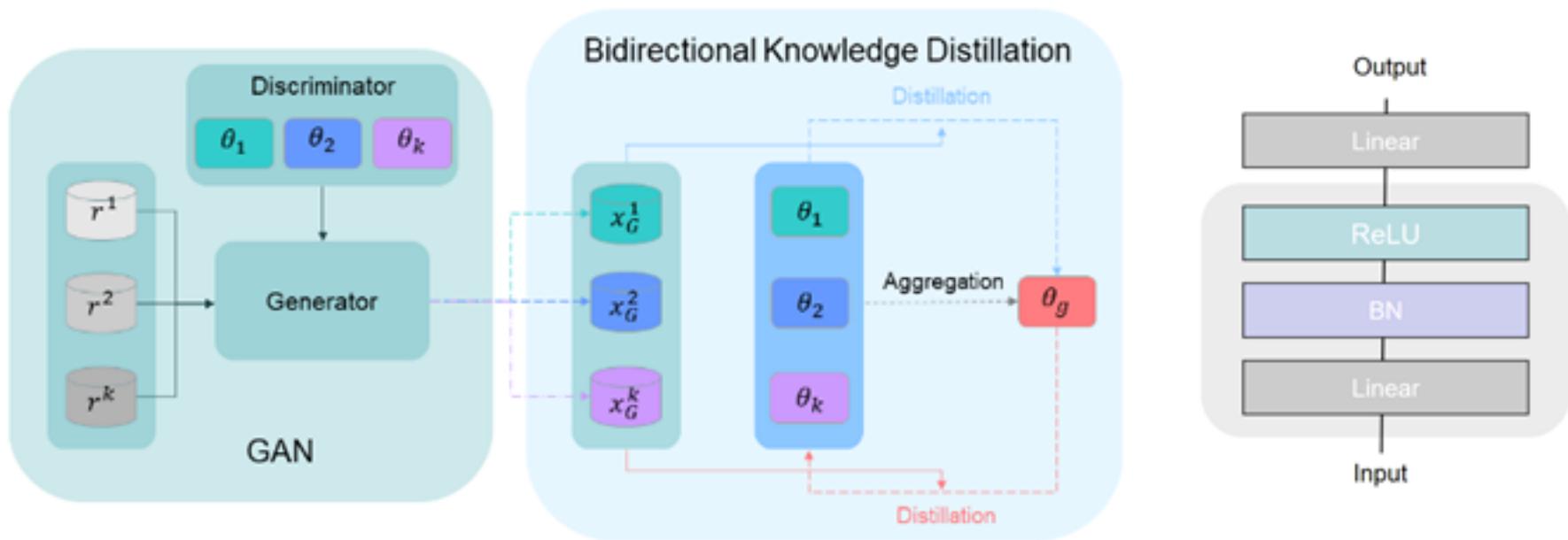
FedCoSR (2024)



- Học representation chia sẻ bằng contrastive loss, giữ head classifier cá nhân. Kết hợp cross-entropy và contrastive loss để thu được embedding ổn định.
- Ưu điểm: Giảm divergence; embedding robust; tốt cho feature shift, các representation được học phù hợp để phân biệt kiểu mã hóa khác nhau trong từng mạng cục bộ.

<https://arxiv.org/abs/2404.17916>

FedBKD (2025)



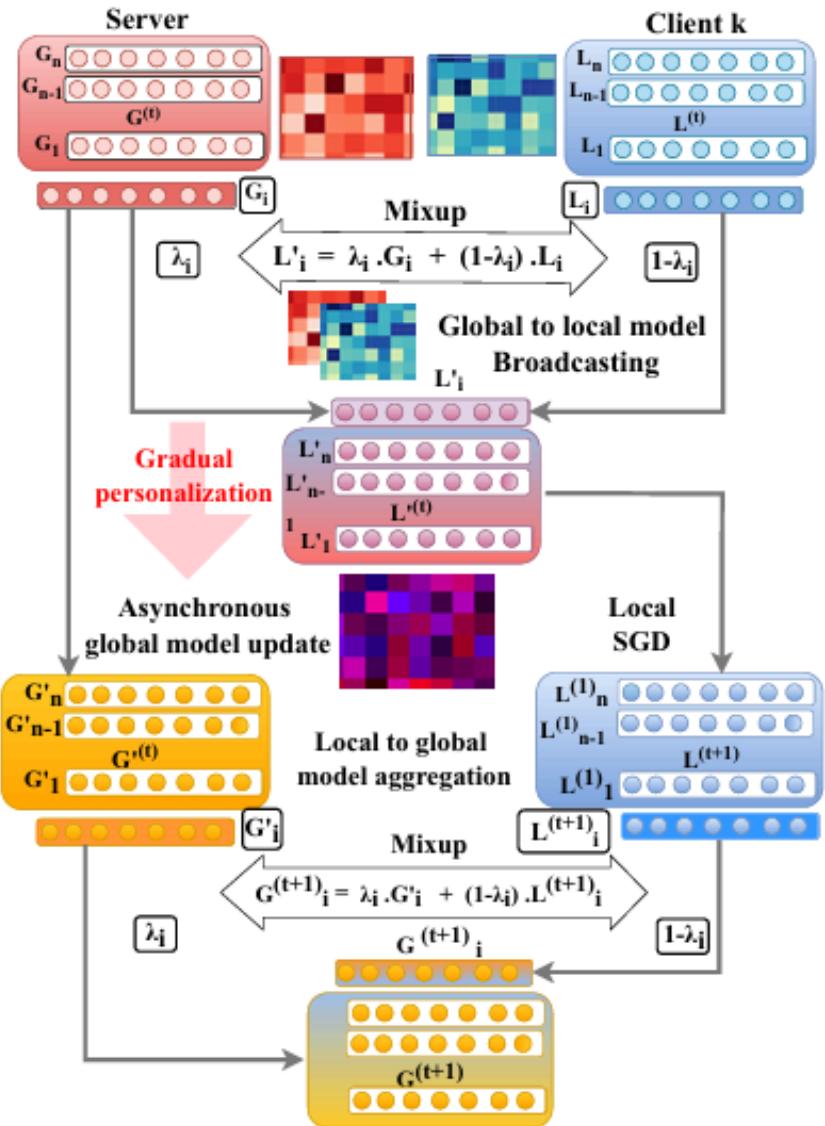
- Kết hợp Knowledge Distillation (KD) trong FL, Clients gửi đi các logits thay vì weights; server sẽ chắt lọc knowledge và gửi lại knowledge cho clients để fine-tune.
- Ưu điểm: Bảo mật tốt hơn; cân bằng giữa generalization và personalization; giảm kích thước truyền thông, tăng robustness khi phân loại, giảm leak dữ liệu, phù hợp với SDN đa miền.

<https://arxiv.org/abs/2506.20245>

pMixFed (2025)

- Áp dụng mixup ở từng lớp mạng theo tỉ lệ thích ứng giữa clients để giảm client drift. Trong một số layer, mix activation/gradient giữa clients dựa trên độ tương đồng; điều chỉnh tỉ lệ mix adaptively.
- Ưu điểm: Giảm drift, tăng tốc hội tụ, tiết kiệm băng thông ở FC layer.

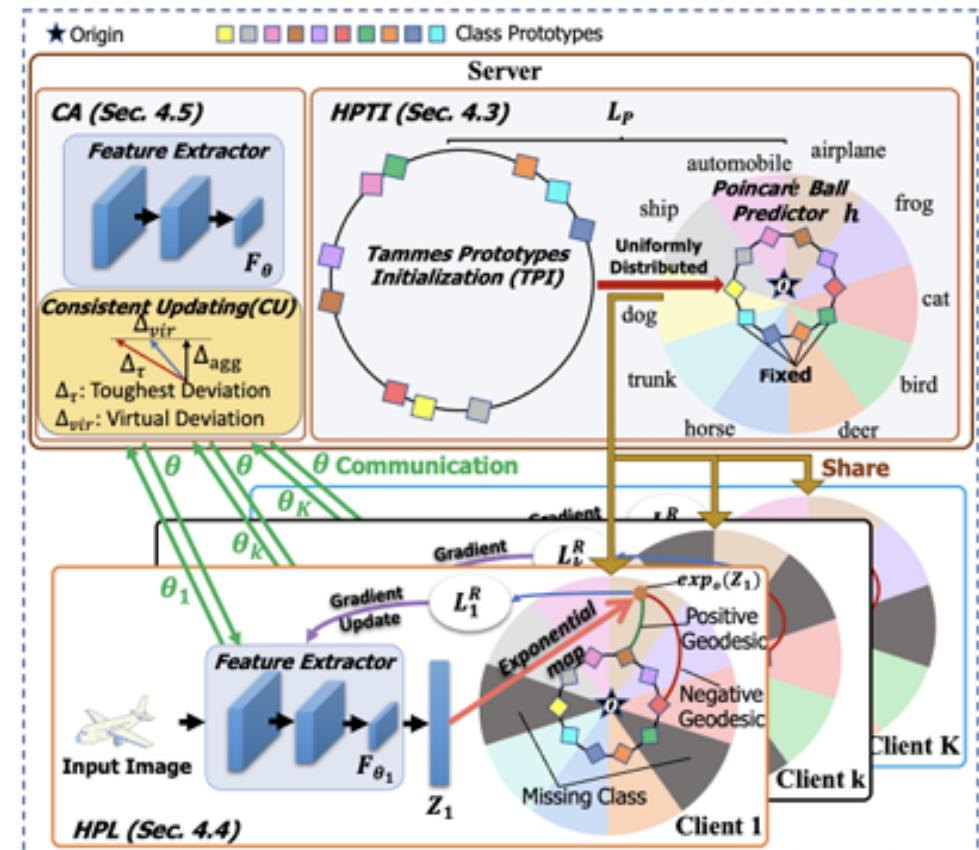
<https://arxiv.org/abs/2501.11002>



HyperFed (2023)

- Sử dụng không gian hyperbolic để lưu prototype class cho dữ liệu phân cấp/đa miền. Prototype được lưu trên manifold hyperbolic;
- Ưu điểm: Biểu diễn tốt cấu trúc phân cấp; ổn định cho dữ liệu phức tạp.

<https://arxiv.org/abs/2307.14384>





HUST

THANK YOU !