

Computação, Saúde e Segurança: Explorando o Potencial da Aprendizagem Federada na Detecção de Arritmias Cardíacas

Arthur N. F. Martins da Costa¹, Pedro Silva¹

¹Departamento de Computação (DECOM) – Universidade Federal de Ouro Preto (UFOP)
Ouro Preto – MG – Brasil

arthur.negrao@aluno.ufop.edu.br, silvap@ufop.edu.br

Abstract. *This article assesses the use of federated learning in the context of cardiac arrhythmia detection. A traditional Deep Learning approach was compared against a federated one, and it was observed that the federated approach was able to maintain predictive performance and training time similar to the original proposal while ensuring the security and privacy of data.*

Resumo. *Este artigo avalia a utilização da aprendizagem federada (federated learning) no âmbito da detecção de arritmias cardíacas. Comparou-se uma abordagem tradicional de Deep Learning contra uma federada, e observou-se que a federada foi capaz de manter desempenho preditivo e tempo de treinamento similares à proposta original ao mesmo tempo que assegura a segurança e privacidade dos dados.*

1. Introdução

A arritmia cardíaca é uma doença que causa a alteração da frequência natural dos batimentos cardíacos, seja por meio da aceleração, desaceleração ou até mesmo irregularidade da mesma. Além de poder dar origem a outras doenças, a própria arritmia pode levar a casos de morte súbita, o que a torna uma verdadeira preocupação para os coordenadores da saúde pública. De acordo com a SOBRAC (Sociedade Brasileira de Arritmias Cardíacas), essa doença atinge mais de 20 milhões de brasileiros e cerca de 320 mil desses vêm a óbito a cada ano [Empresa Brasil de Comunicação 2016].

Em posse de tais informações, compreende-se a importância da realização de diagnósticos rápidos nos estágios iniciais da doença, de forma a evitar a ocorrência de tragédias e fatalidades. Nesse cenário, a inteligência artificial, mais especificamente por meio de *Machine Learning*, surge como uma proposta promissora para solução do problema. Isso porque modelos preditivos na área com altos patamares de desempenho [Rizwan et al. 2020], servem como uma ótima ferramenta auxiliadora para profissionais da área da saúde, facilitando e tornando mais práticos os diagnósticos.

Entretanto, sabe-se que tais modelos tem seu processo de aprendizagem baseado em dados, e, por se tratar de dados médicos, surge uma grande problemática ao redor de sua segurança e privacidade. Como visto no artigo 46º da Lei Geral de Proteção de Dados nº 13.709, os dados de uma pessoa devem ser protegidos para evitar acesso indevido e ilícito [Congresso Nacional 2018]. Dessa forma, o ensino federado surge como uma alternativa, pois permite que um modelos sejam construídos a partir de dados de diferentes entidades sem que as mesmas tenham de compartilhá-los diretamente entre si - evitando vazamentos e garantindo a manutenção de acurácia preditiva.

A aprendizagem federada, em inglês *federated learning*, é uma proposta no ramo de *Machine Learning* onde diversos agentes (por exemplo organizações, indivíduos e/ou empresas) treinam, de maneira colaborativa, um modelo preditivo sob a orquestração de um servidor central mantendo a descentralização dos dados. Ou seja, ao invés de reunir os dados em um ambiente centralizado, cada cliente treina seu modelo individual (utilizando seu subconjunto de dados) e, em momentos determinados pelo servidor, ocorre uma agregação dos parâmetros locais aprendidos. A partir desta agregação, um novo modelo global é disseminado a cada cliente, sendo este processo repetido iterativamente até que se obtenha o desempenho esperado ou um critério de parada seja atingindo. [Kairouz et al. 2021]

Neste trabalho, realizou-se a comparação entre uma proposta tradicional de aprendizado de máquina e uma federada sobre modelos de redes neurais para detecção de presença (ou não) de arritmias cardíacas em sinais de ECG (eletrocardiograma). Ao fim dos experimentos, constatou-se que a proposta federada obteve desempenho levemente superior em termos de acurácia, mais especificamente em cerca de 1% a mais, que a proposta tradicional ao mesmo tempo que manteve a segurança e privacidade dos dados durante o treinamento.

2. Trabalhos relacionados

Esta seção busca apresentar trabalhos sobre detecção de arritmias e as técnicas utilizadas.

Em [Efficient and Intelligent Computing Lab 2022], foi possível observar que uma arquitetura simples - visto que o trabalho era voltado para sistemas embarcados - era capaz de atacar com eficácia o problema, utilizando apenas uma camada convolucional e três camadas densas associadas a técnicas como o *cosine annealing* e *stochastic weight averging*. Os autores atingiram mais de 85% de acurácia no *dataset* da 2022 ACM/IEEE TinyML Design Contest at ICCAD.

Ainda dentro do mesmo *dataset*, observou-se o trabalho proposto em [Zhang et al.], que se dirige ao problema com a transformação dos dados unidimensionais para bidimensionais. Assim, permite-se o processamento dos dados como se fossem “imagens”, permitindo a aplicação dos tradicionais métodos da área que trouxeram bons resultados - atingindo o segundo lugar na competição supracitada.

Por fim, observou-se em [Hanrui Wang] a utilização de técnicas de *ensemble*, onde múltiplos modelos convolucionais unidimensionais “votam” para a decisão da classe de uma determinada instância. Outros fatores interessantes deste trabalho foram o acerto de hiper-parâmetros através da busca *bayesiana* e o tratamento de *outliers*.

Em todos os casos é possível observar a aplicação de técnicas de aprendizado de máquina tradicionais, as quais não se preocupam com a segurança dos dados. O presente trabalho busca avaliar o mesmo conjunto de dados, mas em um contexto federado.

3. Metodologia proposta

O sinal processado neste trabalho possui somente uma dimensão (1D) composto por 1.250 pontos (5 segundos amostrado a 250Hz.), uma vez que representa o sinal cardíaco. Por esse motivo, o modelo foi adaptado para esse contexto. A arquitetura utilizada é sequencialmente composta por: (i) cinco camadas de convolução 1D com *batch normalization* e ativação ReLU; (ii) uma camada *dropout* com 0.5 de probabilidade de ação; (iii) uma

camada densa com 512 neurônios com ativação ReLU; e (iv) uma camada de saída com 2 neurônios utilizando ativação *Softmax*.

A ArrNet (arquitetura utilizada nesse trabalho) foi utilizada para o treinamento federado e tradicional com o otimizador ADAM. A função de perda utilizada foi a *Categorical Crossentropy*. Para a experimentação do modelo federado, os dados são divididos de forma estratificada entre todos os clientes. Já a divisão dos dados foi feita para que 40% do conjunto de dados estivesse presente em cada cliente, permitindo portanto, a repetição de instâncias entre clientes. Apesar de haver possíveis repetições, há uma diversidade de dados considerável entre clientes.

Para a avaliação dos modelos treinados, quatro métricas são utilizadas, sendo elas: acurácia (*ACC*), precisão (*PRE*) e revocação (*REC*). Elas podem ser definidas matematicamente como:

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad PRE = \frac{TP}{TP+FP} \quad REC = \frac{TP}{TP+FN}, \quad (1)$$

onde, *TP* são as classificações de arritmias como arritmias, *TN* são batimentos normais (BN) classificados como BN, *FP* são os BN classificados como arritmias e *FN* são arritmias classificados como BN. Além das métricas supracitadas, também foi empregada a AUC (*Area Under the Curve*) para avaliação do modelo.

4. Experimentos e Resultados

Os experimentos federados foram realizados por meio de três clientes dentro de uma mesma rede local, equipados com: **Cliente 1:** Intel I7-5820k 3.3GHz; GPU TitanXP 12Gb; RAM DDR4 12GB; **Cliente 2:** Intel I9-10900 2.80GHz; GPU RTX 3090 24GB; RAM DDR4 128GB; e **Cliente 3:** AMD Ryzen Threadripper 3960X 3.70GHz; GPU RTX 3090 24GB; RAM DDR4 128GB. O experimento com a abordagem tradicional de *Deep Learning* utilizou a máquina referente ao cliente 3. O modelo ArrNet foi treinado por 30 épocas no contexto tradicional, enquanto que no contexto do treinamento federado ocorreu por 10 épocas locais e 3 globais, utilizando *batch-size* de 32 itens e *learning rate* de 10^{-3} . Utilizou-se o *framework* PyTorch em conjunto com o Flower para o aprendizado federado e o *Scikit-Learn* para o cálculo das métricas.

O *dataset* utilizado foi o disponibilizado na 2022 ACM/IEEE TinyML Design Contest at ICCAD, uma competição realizada pela *International Conference on Computer-Aided Design*. A proposta da competição era construir um modelo baseado em inteligência artificial para sistemas embutidos capaz de realizar a detecção de arritmias cardíacas. O *dataset* consta com 24.589 entradas de treino e 5.626 entradas de teste, onde cada entrada é uma gravação de 5 segundos com amostragem de 250Hz de dados ECG associada a um rótulo que diz se há (1) ou não (0) presença de arritmia cardíaca com risco de vida.

4.1. Resultados

A Tabela 1 apresenta os resultados obtidos com o modelo ArrNet, onde cada coluna indica a média da métrica de avaliação sobre cada uma das 3 execuções de cada método. Com base nestes resultados, é possível observar que o modelo federado desempenhou melhor em todas métricas com exceção do tempo, em média, 20 segundos pior. Apesar de não ser possível estatisticamente generalizar que para todos os casos essa melhora de desempenho se manterá, é possível afirmar que a proposta federada consegue manter um ótimo desempenho preditivo na tarefa de classificação de arritmia ou não. Vale ressaltar

que o modelo ArrNet foi treinado somente com os dados de treino em ambos os paradigmas (tradicional e federado) e que o modelo resultante foi testado nos dados de teste, ou seja, os dados de teste nunca foram vistos pelo ArrNet.

	AUC (%)	ACC (%)	PRE (%)	REC (%)	Tempo (s)
Tradicional	96.09 ± 0.001	94.72 ± 0.003	94.72 ± 0.003	94.67 ± 0.003	158.63 ± 1.41
Federado	96.31 ± 0.003	95.71 ± 0.006	95.55 ± 0.005	95.01 ± 0.005	181.18 ± 2.62

Tabela 1. Resultado Médio dos 3 Treinamentos

Analisando os resultados obtidos, foi possível observar que o modelo proposto, tanto no âmbito centralizado quanto federado, desempenhou, de maneira geral, melhor que os trabalhos relacionados apresentados. Em termos mais precisos, essa diferença atingiu o patamar de 10% sob a métrica de acurácia em comparação ao modelo visto em [Efficient and Intelligent Computing Lab 2022]. Tal fato pode ser explicado principalmente pela inexistência das limitações de *hardware* nos testes realizados, que permitiram a construção de um modelo mais complexo e, conseqüentemente, mais eficaz.

Ademais, vale ressaltar os ganhos em quesito de privacidade e segurança de dados que essa proposta assegurou, já que em momento algum foi necessário o transporte de dados sensíveis entre os nós integrantes da rede federada. Demonstra-se, portanto, um avanço significativo na preservação da confidencialidade das informações, garantindo um ambiente mais seguro e respeitando rigorosamente as questões de proteção de dados sensíveis. Ao mesmo tempo também se constrói um ambiente propício para o desenvolvimento coletivo na área de *Machine Learning/Deep Learning*, com modelos cada vez mais generalizados - visto o treinamento com dados de fontes e realidades diversas.

5. Conclusão

Este estudo demonstra que propostas de aprendizado federado podem ser utilizadas para garantir poder preditivo e segurança de dados nos desafios atrelados às arritmias cardíacas, e, potencialmente, para outros diversos desafios da saúde pública. Para pesquisas e trabalhos futuros, alguns problemas permanecem em aberto, como a expansão dos sistemas federados a novos contextos médicos e o incremento de complexidade destes sistemas, de forma que os mesmos possam auxiliar em diagnósticos médicos de maneiras mais incisivas, com agregação de um maior contingente de informações.

Referências

- Congresso Nacional (2018). Lei nº 13.709, de 14 de agosto de 2018.
- Efficient and Intelligent Computing Lab (2022). Tinymml-contest-solution (GitHub).
- Empresa Brasil de Comunicação (2016). Arritmias cardíacas causam 320 mil mortes súbitas por ano, alerta entidade.
- Hanrui Wang, J. H. iccad-tinymml-open (repositório github).
- Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., et al. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1–2):1–210.
- Rizwan, A., Zoha, A., Mabrouk, I. B., Sabbour, H. M., Al-Sumaiti, A. S., Alomainy, A., Imran, M. A., and Abbasi, Q. H. (2020). A review on the state of the art in atrial fibrillation detection enabled by machine learning. *IEEE reviews in biomedical engineering*, 14:219–239.
- Zhang, J., Chaoyao Shen, X. C., Yuning Ji, Y. Z., et al. Iccad-tinymml-2nd-place (GitHub).