
Formulario de aprobación de curso de posgrado/educación permanente

Asignatura: Aprendizaje Automático para Redes de Datos.-

(Si el nombre contiene siglas deberán ser aclaradas)

Modalidad: **Posgrado**

(posgrado, educación permanente o ambas)

Educación permanente

Profesor de la asignatura ¹: Dr. Ing. Pedro Casas, Investigador Senior, Austrian Institute of Technology, Viena, Austria.

(título, nombre, grado o cargo, instituto o institución)

Profesor Responsable Local ¹: Dr. Ing. Federico La Rocca, Gr. 4, IIE, Facultad de Ingeniería

(título, nombre, grado, instituto)

Otros docentes de la Facultad:No

(título, nombre, grado, instituto)

Docentes fuera de Facultad:No

(título, nombre, cargo, institución, país)

¹ Agregar CV si el curso se dicta por primera vez.

(Si el profesor de la asignatura no es docente de la Facultad se deberá designar un responsable local)

[Si es curso de posgrado]

Programa(s) de posgrado: Maestría y Doctorado en Ingeniería Eléctrica, DET.-

Instituto o unidad: IIE, Facultad de Ingeniería

Departamento o área: Telecomunicaciones

Horas Presenciales: 15

(se deberán discriminar las horas en el ítem Metodología de enseñanza)

Nº de Créditos: 4

[Exclusivamente para curso de posgrado]

(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem Metodología de enseñanza)

Público objetivo: Estudiantes de Posgrado en temas relacionados con la temática del curso, estudiantes del diploma de especialización en telecomunicaciones, profesionales interesados en el área de monitoreo y análisis de redes de datos.

Cupos: No tiene cupo

(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Asimismo, se adjuntará en nota aparte los fundamentos de los cupos propuestos. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción, hasta completar el cupo asignado)

Objetivos:

La popularidad de la Inteligencia Artificial (IA) – y del Aprendizaje Automático/Machine Learning (ML) como un enfoque a la IA, se ha incrementado dramáticamente en los últimos años debido a su excelente desempeño, en particular en el procesamiento de imágenes, audio y lenguaje natural, y más recientemente en gaming.

A pesar de la extensa literatura y varios esfuerzos en integrar los conceptos de IA/ML en redes de datos, su aplicación ha sido menos exitosa en networking. Existe una brecha notable entre la amplia investigación académica en IA/ML para redes de datos y la aplicación de soluciones basadas en IA/ML en entornos operativos. Lo cierto es, que la aplicación de IA/ML en networking presenta varios desafíos que hacen de la misma una tarea altamente compleja.

En este curso abordamos el problema de la aplicación de IA/ML a distintos problemas relacionados con el análisis de redes de datos, incluyendo seguridad en redes, monitoreo de performance, detección de anomalías y calidad de experiencia (QoE). El curso abarca una introducción a los conceptos básicos de ML, así como también un resumen sobre técnicas de ML más recientes, incluyendo aprendizaje profundo, aprendizaje en condiciones adversarias, redes adversarias generativas, IA explicable, etc. Al mismo tiempo, se introducen distintas plataformas Big Data, que permiten el análisis de las cantidades de datos masivas que involucra el monitoreo y análisis de redes de datos.

Conocimientos previos exigidos:

El estudiante debe tener conocimiento de los conceptos básicos de redes de telecomunicaciones, así como también manejar conceptos básicos de matemáticas y estadística.

Conocimientos previos recomendados:

Experiencia previa en análisis estadístico de datos, monitoreo de redes, y aprendizaje automático es altamente recomendable.

Metodología de enseñanza:

(comprende una descripción de la metodología de enseñanza y de las horas dedicadas por el estudiante a la asignatura, distribuidas en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

Descripción de la metodología:

[Obligatorio]

El curso se desarrolla a lo largo de 4 clases, y está conformado por 4 módulos temáticos que abarcan las dos áreas principales, incluyendo aprendizaje automático e inteligencia artificial (módulos 1 y 2), y su aplicación a problemas de redes de datos (módulos 3 y 4).

Las clases se basan en múltiples presentaciones sobre las temáticas planteadas, con un fuerte énfasis en el campo aplicado y en la experiencia del instructor en el área industrial de la aplicación del análisis de datos en redes operacionales.

El enfoque del curso es dinámico y se intentará adaptar a los intereses científicos y/o profesionales de los participantes, a través de ejemplos concretos y de identificación de problemas de interés práctico.

Detalle de horas:

- Horas de clase (teórico):12
- Horas de clase (práctico):0
- Horas de clase (laboratorio):0
- Horas de consulta:3
- Horas de evaluación:0
 - Subtotal de horas presenciales:15
- Horas de estudio:0
- Horas de resolución de ejercicios/prácticos:0
- Horas proyecto final/monografía: 45
 - Total de horas de dedicación del estudiante:60

Forma de evaluación:

[Indique la forma de evaluación para estudiantes de posgrado, si corresponde]

[Indique la forma de evaluación para estudiantes de educación permanente, si corresponde]

Monografía asociada al estudio práctico de uno de los temas del curso, utilizando técnicas de aprendizaje automático sobre bases de datos de tráfico y mediciones de Internet disponibles de forma pública en la red – o sets de datos correspondientes a la actividad científica y/o profesional de los participantes. Se intentará evitar el enfoque de replicar directamente resultados científicos previamente publicados, buscando que la monografía tenga un valor científico dentro del área de desarrollo.

Adicionalmente, para aquellos estudiantes interesados, el tutor plantea la posibilidad de desarrollar la monografía con el objetivo de realizar una publicación científica en conferencias o workshops enfocados a los temas del curso (e.g., TMA 2020, PAM 2020, IMC 2020, Big-DAMA 2020, NET-AI 2020, etc.).

Temario:

Módulo 1 - Introducción al Aprendizaje Automático en Redes de Datos I

- Desafíos en AI4NETS
- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning
- Deep Learning

Módulo 2 – Introducción al Aprendizaje Automático en Redes de Datos II

- Ensemble Learning
- Adaptive Learning
- Explainable AI
- Generative Adversarial Networks (GANs)
- Adversarial Learning
- Transfer Learning y AutoML

Módulo 3 - Aprendizaje Automático y Big Data en Aplicaciones de Redes de Datos

- Plataformas de Big Data Analytics
- Aplicaciones I: AISEC – Seguridad en Redes
- Aplicaciones II: AIPerf – Monitoreo y Detección de Anomalías

- Aplicaciones III: AIQ – Calidad de Experiencia (QoE)

Módulo 4 – Ejemplos de Sistemas basados en Aprendizaje Automático para Redes

- ADAM – Short Memory Continual Learning
- PENSIEVE – Neural Adaptive Video Streaming with Reinforcement Learning
- RAL – Stream Active Learning with Reinforcement
- XAIClust – Explainable AI for Clustering
- GML – Generic ML through Super Learning
- UNADA – Sub-space Clustering for Unsupervised Anomaly Detection

Bibliografía:

(título del libro-nombre del autor-editorial-ISBN-fecha de edición)

Ian Goodfellow, Yoshua Bengio, and Aaron Courville. "**Deep Learning**". MIT Press, 2016.

Raouf Boutaba, Mohammad A. Salahuddin, Noura Limam, Sara Ayoubi, Nashid Shahriar, Felipe Estrada-Solano, and Oscar M. Caicedo. "**A Comprehensive Survey on Machine Learning for Networking: Evolution, Applications and Research Opportunities**". Journal of Internet Services and Applications, 9(1):16, Jun 2018.

A. D'Alconzo, I. Drago, A. Morichetta, M. Mellia, P. Casas, "**A Survey on Big Data for Network Traffic Monitoring and Analysis**". IEEE Transactions on Network and Service Management, 2019.

Robin Sommer and Vern Paxson. "**Outside the Closed World: On Using Machine Learning for Network Intrusion Detection**". In Proceedings of the 2010 IEEE Symposium on Security and Privacy, SP '10, pages 305-316, Washington, DC, USA, 2010. IEEE Computer Society.

Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. "**Why Should I Trust You? Explaining the Predictions of Any Classifier**". In Proceedings of the 22Nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '16, pages 1135-1144, New York, NY, USA, 2016. ACM.

David D. Clark, Craig Partridge, J. Christopher Ramming, and John T. Wroclawski. "**A Knowledge Plane for the Internet**". In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, pages 3-10, New York, NY, USA, 2003. ACM.

Qusay Mahmoud. "**Cognitive Networks: Towards Self-Aware Networks**". Wiley-Interscience, New York, NY, USA, 2007.

Christopher M. Bishop. "**Pattern Recognition and Machine Learning**", 5th Edition. Information science and statistics. Springer, 2007.

Material Adicional de Referencia I (AI4NETS):

R. W. Thomas, L. A. DaSilva, and A. B. MacKenzie. "**Cognitive networks**". In First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005, pages 352-360, Nov 2005.

M. A. Alsheikh, S. Lin, D. Niyato, and H. Tan. "**Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications**". IEEE Communications Surveys Tutorials, 16(4):1996-2018, 2014.

M. Bkassiny, Y. Li, and S. K. Jayaweera. "**A Survey on Machine-Learning Techniques in Cognitive Radios**". IEEE Communications Surveys Tutorials, 15(3):1136-1159, 2013.

A. L. Buczak and E. Guven. "**A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection**". IEEE Communications Surveys Tutorials, 18(2):1153-1176, 2016.

Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani. "**State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrows Intelligent Network Traffic Control Systems**". IEEE Communications Surveys Tutorials, 19(4):2432-2455, 2017.

P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza. "**A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks**". IEEE Communications Surveys Tutorials, 19(4):2392-2431, 2017.

T. T. T. Nguyen and G. Armitage. "**A Survey of Techniques for Internet Traffic Classification using Machine Learning**". IEEE Communications Surveys Tutorials, 10(4):56-76, 2008.

J. Saxe, R. Harang, C. Wild, and H. Sanders. "A **Deep Learning Approach to Fast, Format-Agnostic Detection of Malicious Web Content**". In 2018 IEEE Security and Privacy Workshops (SPW), pages 8-14, 2018.

Benjamin J. Radford, Leonardo M. Apolonio, Antonio J. Trias, and Jim A. Simpson. "**Network Traffic Anomaly Detection Using Recurrent Neural Networks**". CoRR, abs/1803.10769, 2018.

Gonzalo Marin, Pedro Casas, and German Capdehourat. "**DeepSec Meets RawPower - Deep Learning for Detection of Network Attacks Using Raw Representations**". ACM SIGMETRICS Perform. Eval. Rev., 46(3):147-150, January 2019.

P. Casas, P. Mulinka, J. Vanerio, "Should I (re)Learn or Should I Go(on)? **Stream Machine Learning for Adaptive Defense against Network Attacks**", in 26th ACM Conference on Computer and Communications Security (CCS), 6th ACM Workshop on Moving Target Defense (MTD), 2019

S. Wassermann, T. Cuvelier, P. Mulinka, P. Casas, "ADAM & RAL: **Adaptive Memory Learning and Reinforcement Active Learning for Network Monitoring**", in International Conference on Network and Service Management (CNSM), 2019.

P. Casas, J. Vanerio, K. Fukuda, "GML **Learning, A Generic Machine Learning Model for Network Measurements Analysis**", in Proceedings of the 13th International Conference on Network and Service Management (CNSM), 2017.

J. Zhao, S. Shetty, and J. W. Pan. "**Feature-based Transfer Learning for Network Security**". In MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), pages 17-22, 2017.

Wenbo Guo, Dongliang Mu, Jun Xu, Purui Su, Gang Wang, and Xinyu Xing. "**LEMNA: Explaining Deep Learning Based Security Applications**". In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS'18, pages 364-379, New York, NY, USA, 2018. ACM.

Nguyen Cong Luong, Dinh Thai Hoang, Shimin Gong, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. "**Applications of Deep Reinforcement Learning in Communications and Networking: a Survey**". CoRR, abs/1810.07862, 2018.

Hongzi Mao, Mohammad Alizadeh, Ishai Menache, and Srikanth Kandula. "**Resource Management with Deep Reinforcement Learning**". In Proceedings of the 15th ACM Workshop on Hot Topics in Networks, HotNets '16, pages 50-56, New York, NY, USA, 2016. ACM.

Hongzi Mao, Ravi Netravali, and Mohammad Alizadeh. "**Neural Adaptive Video Streaming with Pensieve**". In Proceedings of the Conference of the ACM Special Interest Group on Data Communication, SIGCOMM '17, pages 197-210, New York, NY, USA, 2017. ACM.

Albert Mestres, Alberto Rodriguez-Natal, Josep Carner, Pere Barlet-Ros, Eduard Alarcon, Marc Sole, Victor Munes-Mulero, David Meyer, Sharon Barkai, Mike J. Hibbett, Giovanni Estrada, Khaldun Maruf, Florin Coras, Vina Ermagan, Hugo Latapie, Chris Cassar, John Evans, Fabio Maino, Jean Walrand, and Albert Cabellos. "**Knowledge-Defined Networking**". SIGCOMM Comput. Commun. Rev., 47(3):2-10, September 2017.

Junchen Jiang, Vyas Sekar, Ion Stoica, and Hui Zhang. "**Unleashing the Potential of Data-Driven Networking**". In Communication Systems and Networks - 9th International Conference, COMSNETS 2017, Bengaluru, India, January 4-8, 2017, Revised Selected Papers and Invited Papers, pages 110-126, 2017.

J. Crowcroft. "**Internet Failures: an Emergent Sea of Complex Systems and Critical Design Errors?**" The Computer Journal, 53(10):1752-1757, Dec 2010.

Pavol Mulinka, Sarah Wassermann, Gonzalo Marin, and Pedro Casas. "**Remember the Good, Forget the Bad, do it Fast: Continuous Learning over Streaming Data**". In Advances in Neural Information Processing Systems 32, Continual Learning Workshop, 2018.

Michael L. Brodie, editor. **Making Databases Work: The Pragmatic Wisdom of Michael Stonebraker**. Association for Computing Machinery and Morgan Claypool, New York, NY, USA, 2019.

Andreas Blenk, Patrick Kalmbach, Wolfgang Kellerer, and Stefan Schmid. "**O'Zapft is: Tap Your Network Algorithm's Big Data!**" In Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks, Big-DAMA '17, pages 19-24, New York, NY, USA, 2017. ACM.

Jeffrey Dean, Greg Corrado, Rajat Monga, Kai Chen, Matthieu Devin, Mark Mao, Marc Aurelio Ranzato, Andrew Senior, Paul Tucker, Ke Yang, Quoc V. Le, and Andrew Y. Ng. "**Large Scale Distributed Deep Networks**". In F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, editors, Advances in Neural Information Processing Systems 25, pages 1223-1231. Curran Associates, Inc., 2012.

Andrew Crotty, Alex Galakatos, and Tim Kraska. "**Tupleware: Distributed machine learning on small clusters**". IEEE Data Eng. Bull., 37(3):63-76, 2014.

Erfan Zamanian, Carsten Binnig, Tim Kraska, and Tim Harris. "**The End of a Myth: Distributed Transaction Can Scale**". PVLDB, 10(6):685-696, 2017.

D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. "**Software-Defined Networking: A Comprehensive Survey**". Proceedings of the IEEE, 103(1):14-76, Jan 2015.

Teemu Kopenen, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy, Kye Hyun Kim, Scott Shenker, and Ion Stoica. "**A data-oriented (and beyond) network architecture**". In Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '07, pages 181-192, New York, NY, USA, 2007. ACM.

Michael Mehari. "**Performance Optimization and Modelling of Complex Wireless Networks Using Surrogate Models**". Ghent University, Faculty of Engineering and Architecture, Ghent, Belgium, 2018.

Material Adicional de Referencia II (Learning):

Yann LeCun, Yoshua Bengio, and Geoffrey E. Hinton. "**Deep Learning**". Nature, 521(7553):436-444, 2015.

Juergen Schmidhuber. "**Deep Learning in Neural Networks: an Overview**". Neural Networks, 61:85-117, 2015.

R. R. Salakhutdinov G. E. Hinton. "**Reducing the Dimensionality of Data with Neural Networks**". Science, 313(5786):504-507, July 2006.

Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. "**ImageNet Classification with Deep Convolutional Neural Networks**". In F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, editors, Advances in Neural Information Processing Systems 25, pages 1097-1105. 2012.

Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. "**Generative Adversarial Nets**". In Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, editors, Advances in Neural Information Processing Systems 27, pages 2672-2680. 2014.

Scott M Lundberg and Su-In Lee. "**A Unified Approach to Interpreting Model Predictions**". In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, editors, Advances in Neural Information Processing Systems 30, pages 4765-4774. Curran Associates, Inc., 2017.

Y. Bengio, A. Courville, and P. Vincent. "**Representation Learning: A Review and New Perspectives**". IEEE Transactions on Pattern Analysis and Machine Intelligence, 35(8):1798-1828, Aug 2013.

Asja Fischer and Christian Igel. "**Training Restricted Boltzmann Machines: an Introduction**". Pattern Recognition, 47(1):25-39, 2014.

Vincent Francois-Lavet, Peter Henderson, Riashat Islam, Marc G. Bellemare, and Joelle Pineau. "**An Introduction to Deep Reinforcement Learning**". CoRR, abs/1811.12560, 2018.

German Ignacio Parisi, Ronald Kemker, Jose L. Part, Christopher Kanan, and Stefan Wermter. "**Continual Lifelong Learning with Neural Networks: A Review**". CoRR, abs/1802.07569, 2018.

Ian Goodfellow, Patrick McDaniel, and Nicolas Papernot. "**Making Machine Learning Robust Against Adversarial Inputs**". Commun. ACM, 61(7):56-66, June 2018.

Jacob V. Bouvrie. "**Hierarchical Learning: Theory with Applications in Speech and Vision**". MIT Press, 2009.

R. Caruana. "**Multitask Learning**". Machine Learning, 28(1):41-75, Jul 1997.

Christiane Lemke, Marcin Budka, and Bogdan Gabrys. "**Metalearning: a Survey of Trends and Technologies**". Artificial Intelligence Review, 44(1):117-130, Jun 2015.

Stuart J. Russell and Peter Norvig. "**Artificial Intelligence - A Modern Approach** (3. internat. ed.). Pearson Education, 2010.

Richard S. Sutton and Andrew G. Barto. "**Reinforcement learning - an Introduction**". Adaptive computation and machine learning. MIT Press, 1998.



Facultad de Ingeniería Comisión Académica de Posgrado

Datos del curso

Fecha de inicio y finalización: 2.12.19 – 5.12.19

Horario y Salón: A confirmar

Arancel:

[Si la modalidad no corresponde indique "no corresponde". Si el curso contempla otorgar becas, indíquelo]

Arancel para estudiantes inscriptos en la modalidad posgrado: No corresponde.

Arancel para estudiantes inscriptos en la modalidad educación permanente: 2000 UI
