CEFET/RJ
UnED Petrópolis

DEFESAS DE TCC – 2023/1

ENGENHARIA DE COMPUTAÇÃO

#	Data	Início	Local	Título	Aluno	Orientadores
1	20/06/23	14:00	Sala 102	**Análise do Tráfego de Redes em Jogos Multiplayer**	**Rayssa Cecilia Alves Vilaça**	Dalbert Matos Mascarenhas
	RESUMO: A indústria de jogos movimenta bilhões de dólares anualmente, e um dos fatores que torna os jogos tão viciantes é a capacidade de cativar os usuários através de ambientes virtuais envolventes. Quanto mais imersivo for o jogo, maior será o tempo dedicado pelos jogadores. No entanto, nos jogos multiplayer online, existem desafios que podem prejudicar a experiência, tais como restrições de largura de banda, atrasos na transmissão de dados e variações na latência, afetando negativamente a jogabilidade. Diante dessa realidade, este trabalho realiza uma análise dos impactos negativos causados por tais problemas na experiência dos jogadores durante partidas mul-tiplayer. Com esse propósito em mente, uma versão multiplayer do jogo Pong é desenvolvida, permitindo …					**PALAVRAS-CHAVE:** Jogos Multiplayer, Efeitos Negativos, Tráfego de Redes, Experiência dos Jogadores
2	26/06/23	14:00	Sala 102	**Segmentação e clusterização de anomalias em oleodutos subaquáticos**	**Caio Emiliano Rodrigues e Marcus Vinicius Rosa de Oliveira**	Diego Barreto Haddad (orientador) Fernanda Duarte Vilela Reis de Oliveira
	RESUMO: A segmentação e clusterização de anomalias em oleodutos subaquáticos contribui para a detecção precisa e eficiente de áreas problemáticas, permitindo a tomada de medidas preventivas e a manutenção adequada dos oleodutos, evitando danos ambientais e prejuízos econômicos. O estudo demonstra a aplicação bem-sucedida de técnicas de segmentação e clusterização de oleodutos, evidenciando seu potencial para outras áreas de análise de imagens subaquáticas. Uma base de dados composta por 34.323 imagens, obtidas por meio de inspeção ROV e anotadas com a posição do oleoduto, foi construída. A segmentação das imagens foi realizada utilizando a ferramenta Detectron 2, enquanto a clusterização das anomalias foi conduzida por meio dos algoritmos k-means e fuzzy k-means. Foram obtidos resultados satisfatórios, com uma precisão média de aproximadamente 96\% para o conjunto de teste na etapa de segmentação e precisão média de 88% na clusterização via fuzzy k-means. Esse resultado destaca a eficácia da abordagem proposta no processo de identificação e classificação das anomalias nos oleodutos subaquáticos.					**PALAVRAS-CHAVE:** Oleodutos subaquáticos, Visão computacional, Detectron 2, Extração de características, Clusterização
3	26/06/23	16:00	Salão Nobre	**GreedyKS: Uma ferramenta para detecção de drifts em Big Data**	**Thalis Duarte Galeno**	Luís Domingues Tomé jardim Tarrataca (orientador) Douglas de Oliveira Cardoso (Co-orientador)
	RESUMO: Este trabalho apresenta um algoritmo incremental aproximativo capaz de realizar o teste estatístico de Kolmogorov-Smirnov (KS). Este teste tem como objetivo avaliar o quanto uma sequência de dados segue uma distribuição estatística previamente conhecida, sendo muito útil na detecção de mudanças em fluxo de dados (drifts). A detecção de drifts é uma importante tarefa para algoritmos de aprendizado de máquina pois indicam um possível momento para retreinar os modelos. A detecção de drift sem sequências de dados é um problema difícil de resolver por conta das restrições impostas pelo grande volume de dados. Inspirando-se nesses desafios, esse trabalho apresenta o método GreedyKS para detecção dedrifts, explorando o fato de ser não paramétrico, sendo ideal para lidar com fluxos de dados, mantendo a complexidade algorítmica do teste KS original relativamente pequena. O método tem foco no teste KSone-sample, que avalia…					**PALAVRAS-CHAVE:** Fluxo de dados, Aprendizado Incremental, Mudança de Conceito, Detecção de Mudanças.
4	28/06/23	14:30	Salão Nobre	**Implementação de uma ferramenta de defesa contra o ataque de ARP Spoofing**	**Victor Sadeck de Oliveira**	Dalbert Matos Mascarenhas
	RESUMO: Este trabalho visa desenvolver uma ferramenta para detecção e defesa contra o ataque de ARP Spoofing utilizando a linguagem de programação Python e as ferramentas Tshark e Iptables. Visando atingir o objetivo, foi inicialmente realizado uma pesquisa bibliográfica e então deu-se início ao desenvolvimento da ferramenta. O funcionamento da ferramenta para a detecção de um ataque na rede considera o tempo médio de envio de pacotes de ARP Reply na rede e compara esse tempo com o tempo de um ataque executado pelas principais ferramentas de ataque de ARP Spoofing. Após o desenvolvimento da ferramenta, foram realizados testes para avaliar seu desempenho. Esses testes abrangeram a detecção de falsos positivos e falsos negativos, a captura do tempo necessário para detectar o ataque de ARP Spoofinge bloquear o invasor da rede, além da medição do consumo de memória RAM e CPU. Os resultados obtidos nesses testes foram comparados com quatro das principais ferramentas de defesa contra este ataque descritas na literatura. A ferramenta desenvolvida conseguiu alcançar bons resultados …					**PALAVRAS-CHAVE:** Man-in-the-middle, ARP Spoofing, Segurança de Redes

5	03/07/23	14:00	Salão Nobre	**Simulação pandêmica usando aprendizado por reforço**	**Vinicius de Paula Silvestre**	Luís Domingues Tomé jardim Tarrataca
	RESUMO: Este trabalho apresenta um estudo sobre como uma pandemia pode ser simulada utilizando agentes de Reinforcement Learning (RL) e um jogo desenvolvido especificamente para isso utilizando como base modelos epidemiológicos, com foco específico no modelo SEIR. Foi feita uma comparação entre um modelo de jogo que funcionava com jogadores tomando ações completamente aleatórias e um modelo que utilizasse apenas os agentes de RL tomando decisões informadas. A principal aplicação para tal ferramenta ´e a facilitação da aquisição e da transmissão de conhecimento através de uma ferramenta gráfica de entendimento intuitivo. Foi utilizada o framework Stable Baselines 3 juntamente com a biblioteca Gymnasium da OpenAI na linguagem Python para a construção de tal ferramenta.					**PALAVRAS-CHAVE:** Covid-19, Modelo SEIR, Aprendizado por Reforço, Pandemia
6	03/07/23	15:00	Remoto: MSTeams	**Detecção de ataques de phishing em tempo real utilizando algoritmos de aprendizado de máquina**	**João Araújo de Souza**	Dalbert Matos Mascarenhas
	RESUMO: Phishing´é um tipo de ataque cibernético de engenharia social que visa roubar informações de usuários. Com a pandemia de COVID-19 e popularização do modelo de trabalho remoto, o número de ataques cibernéticos aumentou, especialmente os de phishing. Embora diversas soluções anti-phishing existam, como blacklists e heurísticas, os atacantes estão em constante adaptação. Este trabalho propõe um modelo baseado em aprendizado de máquina para detecção em tempo real de ataques de phishing. Foram testados seis algoritmos dentre os quais o melhor resultado foi obtido pelo Random Forest com 99,15% de acurácia.					**PALAVRAS-CHAVE:** Cibersegurança, Aprendizado de Máquina, Phishing, Detecção em tempo real, Redes de Computadores
7	04/07/23	13:00	Salão Nobre	**Modelagem, Otimizações e Análises de Desempenho de um Workflow Científico de Alta Performance**	**Lucas da Cruz Silva**	Pedro Carlos da Silva Lara (orientador) Kary Ann del Carmen Ocaña Gautherot (co-orientadora)
	RESUMO: Experimentos científicos em larga escala são considerados complexos devido à modelagem de suas atividades, execução e análises de grandes volumes de dados. Na bioinformática esses experimentos são modelados como workflows científicos utilizando conceitos de computação de alto desempenho e ciência de dados. O presente trabalho apresenta o desenvolvimento, otimizações e análises de desempenho de um workflow científico, chamado ParslRNA-seq. Para isso foi utilizado um caso de estudo de expressão diferencial de genes em experimentos de sequenciamento RNA, da bioinformática. As análises exploram o desempenho do workflow com o uso de técnicas de paralelismo como threads, paralelismo de tasks e paralelismo de dados. Além disso, também é realizada uma exploração do desempenho no uso do sistema de arquivos paralelos disponível (Lustre) e no uso de armazenamento local, que conta com SSDs (Solid State Disk), para realização de escrita e leitura de dados. As metodologias aplicadas levaram o ParslRNA-seq a sair de execuções que duravam cerca de 3 dias, para, aproximadamente, 11 horas sem uso de paralelismo…					**PALAVRAS-CHAVE:** workflows científicos, computação de alto desempenho, sequenciamento rna, rna-seq, bioinformática.