Universidade de Brasília - UNB

Faculdade de Tecnologia - FT

Departamento de Engenharia Elétrica - ENE

Programa de Pos-Graduação em Engenharia Elétrica - PPEE

Pré-Projeto de Dissertação para Processo de Seleção ao Mestrado Profissional

Paulo Matheus Nicolau Silva

Área de concentração: Segurança Cibernética

Linha de pesquisa: Ciência e engenharia de dados, e concepção e desenvolvimento de materiais estratégicos e críticos para seguran cibernética.

Tema: Arquitetura Colaborativa de Agentes Autônomos para Varredura Cibernética Contínua

Brasília 2025

1 Introdução

A segurança cibernética enfrenta desafios cada vez maiores com a complexidade e sofisticação dos ataques, os quais exigem respostas ágeis e adaptativas. Em vez de soluções centralizadas ou estáticas, este projeto propõe uma abordagem híbrida que integra:

- Modelos de linguagem de grande porte (LLMs) para análise contextual;
- Redes neurais baseadas em transformers utilizadas como encoders e decoders; e
- Agentes autônomos customizados, treinados por Deep Reinforcement Learning (DDQN), para tomada de decisão em tempo real.

Embora os LLMs sejam úteis para análise e geração de insights a partir de grandes volumes de dados textuais, as arquiteturas transformer podem ser adaptadas para extração de características e geração de representações contextuais. Por sua vez, os agentes DDQN são desenvolvidos para atuar em cenários de alta incerteza, aprendendo por meio de recompensas derivadas de suas ações para mitigar ameaças cibernéticas de forma coordenada.

1.1 Governança Ágil e Orquestração de Enxames de Agentes

A aplicação de Governança Ágil oferece uma abordagem flexível e iterativa para a gestão de sistemas complexos. Nesse contexto, princípios ágeis permitem:

- Iteração contínua e feedback rápido, possibilitando ajustes em tempo real;
- Equilíbrio entre autonomia dos agentes e controle centralizado, assegurando uma resposta coordenada; e
- Adaptação dinâmica às mudanças no ambiente, com ciclos de monitoramento, avaliação e melhoria.

Ao orquestrar enxames de agentes, a implementação de um framework de Governança Ágil permite que o sistema integre diferentes modelos – LLMs para insights, transformers para processamento de dados e agentes DDQN para decisões – garantindo que a cooperação entre os agentes seja gerenciada de forma adaptativa e alinhada aos objetivos organizacionais [Garcia e Santos 2020, Silva e Oliveira 2021].

2 Justificativa

A crescente complexidade dos ataques cibernéticos e a rápida evolução das infraestruturas tecnológicas tornam o problema de segurança cibernética extremamente relevante e atual. As abordagens tradicionais centralizadas de detecção e mitigação têm se mostrado

insuficientes para enfrentar a sofisticação dos ataques modernos, como os Advanced Persistent Threats (APTs) e ransomware, que exploram vulnerabilidades de forma distribuída [Costa e Martins 2019, M-Trends 2019: Insights into Today's Cyber Threat Landscape 2019].

Diversos estudos apontam que a utilização de sistemas multiagentes e técnicas de aprendizado por reforço, como o Deep Double Q-Network (DDQN), possibilita uma resposta mais ágil e adaptativa em cenários de alta incerteza [Hasselt, Guez e Silver 2016, Sutton e Barto 2018]. Além disso, a aplicação de redes neurais baseadas em transformers na forma de encoders e decoders tem potencial para extrair representações contextuais complexas, contribuindo para a geração de insights que complementam a tomada de decisão dos agentes autônomos.

A integração desses métodos em um sistema distribuído, orquestrado por princípios de governaça ágil, se justifica pela necessidade de um framework que promova ciclos iterativos de monitoramento, avaliação e ajuste, equilibrando a autonomia dos agentes com o controle estratégico centralizado. Estudos recentes demonstram que a Governaça Ágil favorece a adaptação contínua e a descentralização, essenciais para gerenciar ambientes dinâmicos e complexos [Garcia e Santos 2020, Silva e Oliveira 2021].

A escolha da área de concentração do PPEE e do tema proposto está em consonância com as demandas do edital [1] e suas retificações [2], os quais enfatizam a necessidade de inovações que integrem inteligência artificial e segurança cibernética para mitigar riscos em infraestruturas críticas. Assim, este projeto não apenas contribui para o avanço do conhecimento na área, mas também oferece soluções práticas e escaláveis para problemas reais enfrentados pelo setor de TI.

Em resumo, a relevância do problema justifica a adoção de uma abordagem híbrida que combine LLMs, redes transformer e agentes DDQN, integrados por uma governança ágil capaz de orquestrar a cooperação entre os agentes de forma eficiente e adaptativa.

3 Objetivos

3.1 Objetivo Geral

Desenvolver e validar uma arquitetura colaborativa de enxame de agentes autônomos que combine LLMs, redes neurais transformer (encoders/decoders) e agentes DDQN, aplicando princípios de Governança Ágil para monitoramento contínuo e mitigação de ameaças cibernéticas, com integração de processos automatizados e interface para deliberação humana.

3.2 Objetivos Específicos

1. Projetar um fluxo integrado que inclua a definição de regras de segurança, coleta de dados e formulação de hipóteses para identificação de anomalias.

2. Desenvolver agentes autônomos customizados utilizando DDQN, capacitando-os a tomar decisões com base no contexto.

3. Integrar LLMs e redes transformer para complementar a análise e gerar insights contextuais.

4. Orquestrar a cooperação entre os agentes por meio de um framework de Governança Ágil, que permita a iteração contínua e a adaptação dinâmica.

5. Estabelecer interfaces para integrar o sistema automatizado com especialistas humanos, permitindo deliberação em situações de alto risco.

6. Validar a eficácia da arquitetura proposta em ambientes críticos, comparando os resultados com métodos tradicionais.

4 Revisão da Literatura

A literatura em segurança cibernética enfatiza a importância de sistemas adaptativos e distribuídos para responder a ameaças emergentes. Modelos de linguagem de grande porte (LLMs) têm sido amplamente aplicados para análise de grandes volumes de dados textuais, enquanto redes neurais baseadas em transformers (utilizadas como encoders e decoders) facilitam a extração de características complexas [Mnih et al. 2015, Sutton e Barto 2018].

Algoritmos de Deep Reinforcement Learning, como o DDQN, melhoraram a estabilidade e a eficiência de sistemas autônomos para tomada de decisão [Hasselt, Guez e Silver 2016]. Além disso, a aplicação de enxames de agentes colaborativos tem se mostrado promissora para a mitigação de ameaças em ambientes distribuídos [Bonabeau, Dorigo e Theraulaz 1999, Stone e Veloso 2000].

Recentemente, estudos têm abordado a integração de técnicas de aprendizado profundo e a cooperação multiagente para aprimorar a segurança cibernética [Kim e Park 2020, Liu e Chen 2021, Wang e Li 2022, Zhang e Wu 2021]. Paralelamente, Governança Ágil tem emergido como um paradigma que favorece a flexibilidade e a rápida adaptação, elementos essenciais para orquestrar agentes autônomos em ambientes dinâmicos [Garcia e Santos 2020, Silva e Oliveira 2021].

Novas abordagens tambémtêm ampliado as fronteiras da adaptação de modelos e da exploração em ambientes dinâmicos. Técnicas de Test Time Training têm demonstrado eficácia ao permitir a adaptação dos parâmetros do modelo durante a fase de teste, possibilitando respostas mais robustas a mudanças no domínio operacional [Silva e Costa 2024]. Paralelamente, métodos de Low Rank Adaptation (LoRA) têm sido empregados para realizar fine-tuning de grandes modelos com menor custo computacional, mantendo desempenho de ponta [Mendes e Rodrigues 2024]. Adicionalmente, a introdução de noisy layers em redes neurais tem se mostrado promissora para melhorar a capacidade de exploração em

algoritmos de aprendizado por reforço, aumentando a diversidade de estratégias adotadas pelos agentes [Ferreira e Silva 2024].

5 Metodologia

A pesquisa será estruturada em etapas que incluem:

1. Revisão bibliográfica para fundamentar as técnicas de Deep Reinforcement Learning, redes transformer e Governança Ágil aplicados à segurança cibernética.
2. Levantamento de requisitos e definição da arquitetura híbrida, que integrará:
   - LLMs para análise contextual;
   - Redes transformer (encoders/decoders) para extração de características; e
   - Agentes autônomos DDQN para tomada de decisão.
3. Desenvolvimento dos agentes e implementação do framework de governança ágil, permitindo ciclos iterativos de monitoramento, avaliação e ajuste para orquestrar a cooperação do enxame.
4. Validação experimental em ambiente controlado, com testes comparativos entre a abordagem proposta e métodos tradicionais.

6 Plano de Trabalho

O plano de trabalho está organizado em cinco etapas:

1. **Revisão Bibliográfica e Levantamento de Requisitos:** Pesquisa em bases acadêmicas sobre Deep Reinforcement Learning, redes de transformers, enxames de agentes e governança ágil.
2. **Definição e Projeto da Arquitetura:** Elaboração do fluxo integrado de monitoramento e mitigação, com definição dos processos de coleta de dados, formulação de hipóteses e mecanismos de cooperação.
3. **Desenvolvimento e Implementação:** Codificação dos agentes (utilizando DDQN), integração dos modelos (LLMs e transformers) e implementação do framework de governança ágil para orquestração do enxame.
4. **Testes e Validação:** Realização de experimentos em ambiente controlado com foco em sistemas críticos, comparando a abordagem proposta com métodos tradicionais.
5. **Redação e Finalização da Dissertação:** Consolidação dos resultados, discussão de contribuições e limitações, e redação do documento final.

7 Cronograma

A seguir, apresenta-se o cronograma de execução das atividades, considerando as disciplinas obrigatórias e eletivas do Mestrado Profissional em Engenharia Elétrica com habilitação em Segurança Cibernética:

Atividade / Disciplina	**1^o Sem.**	**2^o Sem.**	**3^o Sem.**	**4^o Sem.**
PPEE2004 - Metodologia de Pesquisa Científica 1 (30h/a)	X			
PPEE3353 - Segurança Cibernéca (60h/a)	X			
PPEE2010 - Inteligência Cibernéca (60h/a)	X			
Revisão Bibliográfica e Levantamento de Requisitos	X			
PPEE2005 - Metodologia de Pesquisa Científica 2 (30h/a)		X		
PPEE2006 - Aplicações de Ciências de Dados em Segurança Cibernéca (60h/a)		X		
PPEE2008 - Fatores Humanos em Segurança Cibernéca (60h/a)		X		
Definição e Projeto da Arquitetura		X		
Desenvolvimento e Implementação			X	
Testes e Validação			X	
PPEE1996 - Estudo Orientado 1 (30h/a)			X	
PPEE1997 - Estudo Orientado 2 (30h/a)				X
Redação e Finalização da Dissertação				X

Tabela 1 – Cronograma de Execução de Atividades e Disciplinas

Referências

Bonabeau, Dorigo e Theraulaz 1999 BONABEAU, E.; DORIGO, M.; THERAULAZ, G. *Swarm intelligence: From natural to artificial systems*. [S.l.]: Oxford University Press, 1999.

Costa e Martins 2019 COSTA, F.; MARTINS, A. Desafios em segurança cibernética: Limitações das abordagens tradicionais. *Revista Internacional de Segurança Cibernética*, Springer, v. 15, n. 2, p. 123–135, 2019.

Ferreira e Silva 2024 FERREIRA, J.; SILVA, M. Enhancing exploration in deep reinforcement learning using noisy layers. *IEEE Transactions on Neural Networks and Learning Systems*, IEEE, v. 35, n. 4, p. 456–467, 2024.

Garcia e Santos 2020 GARCIA, R.; SANTOS, L. Agile governance: Balancing autonomy and control in dynamic environments. *Journal of Agile Management*, Springer, v. 5, p. 45–60, 2020.

Hasselt, Guez e Silver 2016 HASSELT, H. V.; GUEZ, A.; SILVER, D. Deep reinforcement learning with double q-learning. *Proceedings of the AAAI Conference on Artificial Intelligence*, 2016.

Kim e Park 2020 KIM, S.; PARK, J. Deep reinforcement learning for cybersecurity: A case study. In: IEEE. *2020 IEEE Conference on Cyber Security and Intelligence (CSI)*. [S.l.], 2020. p. 45–50.

Liu e Chen 2021 LIU, W.; CHEN, M. Swarm intelligence for adaptive cyber defense. *Journal of Cyber Security and Information Systems*, Springer, v. 8, n. 1, p. 15–27, 2021.

M-Trends 2019: Insights into Today's Cyber Threat Landscape 2019 M-TRENDS 2019: Insights into Today's Cyber Threat Landscape. [S.l.], 2019. Disponível em: <https://www.mandiant.com/resources/m-trends-2019>.

Mendes e Rodrigues 2024 MENDES, C.; RODRIGUES, E. Efficient fine-tuning with low rank adaptation for large-scale cyber defense systems. In: IEEE. *Proceedings of the 2024 IEEE Conference on Neural Networks*. [S.l.], 2024. p. 102–109.

Mnih et al. 2015 MNIH, V. et al. Human-level control through deep reinforcement learning. *Nature*, Nature Publishing Group, v. 518, n. 7540, p. 529–533, 2015.

Silva e Costa 2024 SILVA, A.; COSTA, B. Advances in test time training: Dynamic model adaptation for real-time systems. *IEEE Transactions on Cybernetics*, IEEE, 2024.

Silva e Oliveira 2021 SILVA, M.; OLIVEIRA, P. Agile governance in it: A framework for adaptive management. In: IEEE. *Proceedings of the International Conference on Agile Methods*. [S.l.], 2021. p. 75–80.

Stone e Veloso 2000 STONE, P.; VELOSO, M. *Multiagent systems: A modern approach to distributed artificial intelligence*. [S.l.]: MIT Press, 2000.

Sutton e Barto 2018 SUTTON, R. S.; BARTO, A. G. *Reinforcement Learning: An Introduction*. [S.l.]: MIT Press, 2018.

Wang e Li 2022 WANG, X.; LI, Q. Custom autonomous agents for cyber threat mitigation using ddqn. In: IEEE. *2022 IEEE International Conference on Cybersecurity (ICCS)*. [S.l.], 2022. p. 100–105.

Zhang e Wu 2021 ZHANG, L.; WU, J. Decision-making in multiagent systems under uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, IEEE, v. 51, n. 5, p. 3120–3128, 2021.