Instituto de Informática (INF)
Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre - RS
URL: https://www.inf.ufrgs.br

Orientador: Prof. Dr. Lisandro Zambenedetti Granville
Coorientador: Dr. Muriel Figueredo Franco
Grupo de Redes de Computadores
E-mail: [granville, mffranco]@inf.ufrgs.br

Inteligência Artificial para Identificação de Comportamentos Maliciosos em Redes de Computadores Programáveis

1 Introdução e Motivação

Redes programáveis permitem que mudanças, tanto no plano de dados quanto no plano de controle, possam alterar o comportamento da comnicação na rede, seus dispositivos, e aplicações [1]. Para isso, softwares de rede podem ser desenvolvidos para alterar ou gerenciar o funcionamento da rede de forma muito mais flexível que os tradicionais dispositivos físicos (*i.e.,* hardware) que implementam os planos de controle e dados de forma fixa. Redes programáveis são parte de uma longa história de evolução em redes de computadores, iniciando com discussões sobre redes ativas e virtualização de rede na década de 90. Porém, em 2008, o paradigma conhecido como Redes Definidas por Software (do inglês Software-Defined Networking – SDN) definiu um caminho incremental e casos de uso bem definidos para tornar possível a programabilidade no mundo corporativo [2]. Porém, SDN não é o final da evolução. Atualmente, SDN está se tornando obsoleto, porém, seus conceitos podem ser aplicados para diferentes tarefas, como por exemplo automação de redes [4], gerenciamento centralizado e outras abordagens que requerem maior flexibilidade e "softwarização" da rede.

Juntamente com a flexibilidade introduzida com o paradigma de redes de computadores programáveis, falhas de segurança e comportamentos maliciosos podem ser detectados de forma automatizada [3]. Diferentes trabalhos na literatura exploram SDN e a linguagem Programming Protocol-Independent Packet Processors (P4) [5, 3] para o desenvolvimento de software de redes capazes de identificar ciberataques. Porém, existe a necessidade (e oportunidade) da utilização de técnicas de

Inteligência Artificial (IA) para a análise de padrões de comportamento de dispositivos e tráfego em redes prográmaveis. Com isso, soluções inteligentes e automatizadas podem ser propostas para garantir comunicações seguras e de alto desempenho para as novas gerações de redes de computadores (*e.g.,* 5G e redes autonômicas).

2 Descrição das Atividades

As atividades a serem desenvolvidas durante o TG1 e TG2 são descritas abaixo. Porém, tais atividades podem ser alteradas de acordo com a necessidade durante o desenvolvimento do trabalho. O trabalho será executado em parceria com a Universidade de Zurique, Suiça. Portanto, o/a aluno(a) poderá optar por orientação em Português ou Inglês.

A1. **Estudo dos conceitos de redes programáveis e técnicas de IA:** Essa atividade deve ser conduzida de modo ao/a aluno(a) familiarizar-se com o tópico do trabalho e seus principais fundamentos. Tópicos chaves para estudo serão discutidas com o orientador nas reuniões iniciais.

A2. **Revisão bibliográfica de segurança e IA para redes programáveis:** Após o entendimento dos conceitos chaves, o/a aluno(a) deverá analisar artigos científicos relacionados a falhas de segurança em redes programáveis, especialmente artigos que utilizem técnicas de IA como possível solução para problemas identificados na área.

A3. **Definição de uma solução automatizada para identificação de comportamentos maliciosos em redes programáveis:** O/A aluno(a) deverá ser capaz, juntamente com os orientadores, de propor uma solução eficaz para resolver problemas previamente identificados na literatura de forma inovadora e eficaz. A solução deverá explorar técnicas de IA para identificação de comportamentos maliciosos em redes programáveis, o qual poderá ser baseado na análise de tráfego, dos dispositivos de rede ou outras métricas identificadas ao longo do trabalho.

A4. **Design e implementação da solução:** A solução proposta deverá ser implementada como prova de conceito. A implementação poderá utilizar diferentes tecnologias e técnicas de engenharia de software previamente definidas com os orientadores.

A5. **Avaliação da solução:** A solução deverá ser analisada de forma quantitativa e/ou qualitativa. As avaliações serão definidas juntamente com os orientadores, de forma a alcançar os melhores resultados possíveis dentro do prazo de execução do trabalho.

A6. **Escrita do Trabalho de Conclusão:** Essa atividade é continua e deverá ser realizada ao longo de todo o trabalho, conforme discussão e cronograma definido com os orientadores. O Trabalho de Conclusão deverá apresentar de forma clara e completa o trabalho proposto e seu desenvolvimento.

As atividades deverão ser realizadas ao longo de 1 (um) ano durante as cadeiras de Trabalho de Graduação (TG) 1 e 2. As atividades de escrita deverão ocorrer em paralelo com o desenvolvimento prático do trabalho. Sugere-se que os seguintes capítulos estejam concluídos ao final de cada uma das cadeiras:

- **TG1**: Introdução e Motivação, Referencial Teórico e Trabalhos Relacionados;
- **TG2**: Abordagem, Implementações, Avaliações e Conclusões.

Porém, tais atividades e entregas poderão ser alteradas se acordadas com os orientadores para um melhor desenvolvimento do trabalho e adequação a metas/resultados do trabalho.

3 Requisitos

- Conceitos básicos de cibersegurança
- Conceitos básicos de IA
- Interesse por redes de computadores;
- Capacidade para leitura de artigos em Inglês (Desejável mas não obrigatório);

References

[1] N. Anerousis, P. Chemouil, A. A. Lazar, N. Mihai, and S. B. Weinstein, "The Origin and Evolution of Open Programmable Networks and SDN," IEEE Communications Surveys & Tutorials, Vol. 23, No. 3, pp. 1956–1971, 2021.

[2] N. Feamster, J. Rexford, and E. Zegura, "The Road to SDN: an Intellectual History of Programmable Networks," ACM SIGCOMM Computer Communication Review, Vol. 44, No. 2, pp. 87–98, 2014.

[3] A. S. Jacobs, A. J. G. de Azambuja, A. E. Schaeffer-Filho, J. C. Nobre, J. A. Wickboldt, L. Z. Granville, L. P. Gaspary, and W. L. da Costa Cordeiro, "Protegendo Redes de Computadores na Era do Plano de Dados Programáveis," Sociedade Brasileira de Computação, 2022.

[4] T. Mai, S. Garg, H. Yao, J. Nie, G. Kaddoum, and Z. Xiong, "In-network Intelligence Control: Toward a Self-driving Networking Architecture," IEEE Network, Vol. 35, No. 2, pp. 53–59, 2021.

[5] R. Parizotto, L. Castanheira, and A. Schaeffer-Filho, "Abordagem de Composição de Programas P4 em Redes Programáveis," Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Porto Alegre, RS, Brasil: SBC, 2019, pp. 1028–1041. [Online]. Available: https://sol.sbc.org.br/index.php/sbrc/article/view/7420