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. Eder John Scheid
Grupo de Redes de Computadores
E-mail: [granville, ejscheid]@inf.ufrgs.br

Extraindo e Identificando Transações Blockchain em Redes Programáveis

1 Introdução e Motivação

Os conceitos de blockchain e a tecnologia Distributed Ledgers (DL) [6] vem sendo amplamente utilizados em uma miríade de aplicações em diversas áreas, *e.g.,* Internet das Coisas (IoT), saúde, cibersegurança, e finanças [4]. Com isso, algumas dessas aplicações necessitam de requisitos diferentes de Qualidade de Serviço (QoS) e desempenho. Por isso, é necessário *(1)* inspecionar pacotes de rede e *(2)* identificar tais aplicações para aplicar políticas de encaminhamento de tráfego ou realizar ações específicas de engenharia de tráfego. Um meio de atingir tais objetivo e realizar engenharia de tráfego é utilizar o conceito de redes programáveis e *Software-Defined Networking (SDN)* para controlar a rede de uma maneira flexível e com visão global [3]. Entretanto, implementar tal inspeção de pacotes utilizando SDN leva a problemas de escalabilidade e latência dado ao envolvimento de um controlador SDN no processo [5]. Portanto, processar pacotes diretamente no plano de dados (*i.e., switches*), evitando assim encaminhar pacotes para o controlador SDN, se torna uma alternativa para resolver tal limitação.

Nesse sentido, linguagens para processar pacotes de maneira programável, como Programming Protocol-independent Packet Processors (P4) [1], podem ser utilizadas para a extração de características e identificação de transações blockchain em nível de processamento de pacotes em *switches* programáveis. Tal programação direta no *switch* pode ser útil para *(i)* identificar dispositivos infectados por *cryptojackers* [2], *(ii)* priorizar e otimizar o tráfego de aplicações blockchain, *e.g.,* mineradores, e *(iii)* balancear a carga para diferentes nós blockchain. Portanto, este trabalho visa explorar tais conceitos e propor uma solução que possa ser utilizada dentro de um ou mais casos de uso da área de blockchain.

2 Descrição das Atividades

Dada a introdução e motivação descrita acima, as seguintes atividades são planejadas para serem desenvolvidas durante o TG1 e TG2. É importante salientar que tais atividades podem ser alteradas durante o desenvolvimento dos trabalhos.

A1. **Estudo dos conceitos e tecnologias envolvidas**. Durante esta primeira etapa, o/a aluno(a) deverá se familiarizar com os conceitos e tópicos envolvidos no trabalho, como blockchain, redes programáveis, SDN, e P4.

A2. **Revisão bibliográfica da área.** Assim que o/a aluno(a) estiver familiarizado com os conceitos principais, ele/ela começará a etapa de investigação e análise de artigos científicos relacionados com o tema afim de mapear o estado-da-arte da área e identificar possíveis problemas e soluções para o mesmo.

A3. **Definição e delimitação do escopo da solução proposta.** Esta etapa compreende a definição dos requisitos e objetivos que deverão ser atingidos pela solução. Sua delimitação deve considerar a pesquisa realizada na etapa anterior afim de propor uma solução inovadora.

A4. **Modelagem e implementação da solução.** A solução proposta deverá ser modelada de uma maneira agnóstica a tecnologia utilizada a para a sua posterior implementação. A implementação da solução se dará como uma prova de conceito levando em conta os requisitos e objetivos listados.

A5. **Avaliação da prova de conceito.** Com a prova de conceito implementada, o/a aluno(a) irá se dedicar a avaliar a mesma em diferentes aspectos que deverão ser discutidos com os orientadores afim de melhor demonstrar sua eficácia.

A6. **Escrita do Trabalho de Conclusão.** Essa atividade é continua e deverá ser realizada ao longo de todo o trabalho conforme discussão 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 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

- Interesse por blockchain e criptomoedas;
- Conhecimento básico de redes de computadores;
- Conhecimento básico de rede programáveis (desejável, mas não obrigatório);
- Inglês técnico (para leitura de artigos científicos).

References

[1] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker, "P4: Programming Protocol-Independent Packet Processors," SIGCOMM Comput. Commun. Rev., Vol. 44, No. 3, pp. 87—-95, July 2014.

[2] A. H. Celdrán, P. M. S. Sánchez, M. A. Castillo, G. Bovet, G. M. Pérez, and B. Stiller, "Intelligent and Behavioral-based Detection of Malware in IoT Spectrum Sensors," International Journal of Information Security, pp. 1–21, July 2022.

[3] N. Feamster, J. Rexford, and E. Zegura, "The Road to SDN: An Intellectual History of Programmable Networks," SIGCOMM Comput. Commun. Rev., Vol. 44, No. 2, p. 87–98, apr 2014.

[4] A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," IEEE Access, Vol. 7, pp. 117 134–117 151, August 2019.

[5] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, and P. Castoldi, "P4 Edge Node Enabling Stateful Traffic Engineering and Cyber Security," J. Opt. Commun. Netw., Vol. 11, No. 1, pp. A84–A95, Jan 2019.

[6] E. J. Scheid, B. Rodrigues, C. Killer, M. Franco, S. Rafati, and B. Stiller, "Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues," Advancing Research in Information and Communication Technology, ser. IFIP AICT Festschrifts. Cham, Switzerland: Springer, 08 2021, Vol. 600, pp. 289–317.