

Proposta para Dissertação de Mestrado em Engenharia Informática

Título:

Deteção de Ataques do Tipo Low-rate DDoS em Redes Definidas por Software Usando Algoritmos de Sketching e de Machine Learning

Orientador:

Mário Freire (email: mario@di.ubi.pt; página web: <http://www.di.ubi.pt/~mario/>)

Sumário

As redes definidas por software (SDN -Software Defined Networking) [1] estão a tornar-se muito atrativas para ambientes virtualizados e centros de dados devido às características de escalabilidade, flexibilidade e monitorização. As redes definidas por software separam o plano de dados do plano de controlo, permitindo a centralização do plano de controlo e a execução de aplicações neste plano, programadas pelo operador, que permitem a conguração automática de equipamentos de encaminhamento. Este tipo de redes permite a utilização de algoritmos de sketching nos switches, que fornecem estatísticas sobre a carga da rede, incluindo estatísticas sobre fluxos. Nesta dissertação pretende-se investigar a deteção de ataques do tipo low-rate DDoS (Distributted Denial of Service) em redes definidas por software recorrendo a algortimos de sketching. Existem alguns artigos recentes que abordam a detecção de ataques do tipo high-rate DDoS em redes definidas por software [2]-[5]. Contudo, tanto quanto é do nosso conhecimento, não há registos na literatura da detecção de ataques do tipo low-rate DDoS em redes definidas por software, que se caracterizam por ter um perfil de tráfego semelhante ao de um utilizador normal e de serem, por isso, difíceis de detectar. Para a deteção de ataques do tipo low-rate DDoS pretende-se investigar a utlização de algoritmos de machine learning, já investigados para detectar ataques do tipo high-rate DDoS em redes de computadores vulgares [6]-[8], em conjunto com algoritmos de sketching, usando o Mininet [9].

Objetivos

O principal objetivo desta dissertação consiste na implementação e avaliação de um método para deteção de ataques do tipo low-rate DDoS em redes definidas por software usando algoritmos de sketching e de machine learning, através do Mininet.

Tarefas a Realizar

São propostas as seguintes tarefas para a execução do trabalho de investigação e de desenvolvimento, conducente à elaboração da dissertação de mestrado:

- Tarefa 1. Estudo dos principais conceitos subjacentes às redes definidas por software.
- Tarefa 2. Estudo dos principais conceitos subjacentes à deteção de ataques DDoS em geral e low-rate DDoS em particular.
- Tarefa 3. Instalação e configuração do ambiente de teste para deteção de ataques do tipo DDoS em redes programáveis no plano de dados.
- Tarefa 4. Implementação e teste do método para deteção de ataques low-rate DDoS em redes definidas por software, usando algoritmos de sketching e de machine learning.
- Tarefa 5. Execução de experiências laboratoriais e produção de resultados experimentais.
- Tarefa 6. Escrita de um artigo científico sobre o trabalho de investigação realizado e escrita da dissertação de mestrado.

Cronograma

A tabela seguinte representa a calendarização prevista para a execução das tarefas, em que a execução de uma dada tarefa num determinado mês é assinalada com um x.

Tarefa/mês	Set 19	Out 19	Nov 19	Dez 19	Jan 20	Fev 20	Mar 20	Abr 20	Mai 20	Jun 20
Tarefa 1	x									
Tarefa 2		x								
Tarefa 3			x	x						
Tarefa 4				x	x	x				
Tarefa 5							x			
Tarefa 6								x	x	x

Escrita da Dissertação em Língua Inglesa

A dissertação de mestrado resultante da realização do plano de trabalho proposto deverá ser escrita em língua inglesa, tendo em vista a divulgação internacional do trabalho científico desenvolvido. O título da dissertação em língua inglesa deverá ser o seguinte: “Detection of Low-rate DDoS Attacks in Software Defined Networks Using Sketching and Machine Learning Algorithms”.

Referências

- [1] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, “Advancing Software-Defined Networks: A Survey”, IEEE Access, Vol. 5, pp. 25487-25526, 2017.
- [2] M. Imran, M. H. Durad, F. A. Khan, and A. Derhab, "Toward an optimal solution against Denial of Service attacks in Software Defined Networks", Future Generation Computer Systems, Vol. 92, pp. 444–453, 2019.
- [3] J. Cui, M. Wanga, Y. Luo, H. Zhong, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN", Future Generation Computer Systems, Vol. 97, pp. 275–283, 2019.
- [4] S. Deng, X. Gaob, Z. Lua, Z. Li , X. Gao, "DoS vulnerabilities and mitigation strategies in software-defined networks", Journal of Network and Computer Applications, Vol. 125, 209–219, 2019.
- [5] A. C. Lapolli, J. A. Marques, and L. P. Gasparry, "Offloading Real-time DDoS Attack Detection to Programmable Data Planes", Proceedings of 2019 IFIP/IEEE International Symposium on Integrated Network Management (IM2019), pp. 19-27.
- [6] Bashar Ahmed Khalaf, Salama A. Mostafa, Aida Mustapha, Mazin Abed Mohammed, And Wafaa Mustafa Abdulllah, "Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods", IEEE Access, Vo. 17, pp. 51691 - 51713, 2019. DOI: 10.1109/ACCESS.2019.2908998
- [7] I. Sreeram and V. P. Ku. Vuppala, "HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm", Applied Computing and Informatics, Vol. 15, pp. 59–66, 2019.
- [8] Muhammad Aamir and Syed Mustafa Ali Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification", Journal of King Saud University – Computer and Information Sciences, In press, 2019.
- [9] Mininet, An Instant Virtual Network on your Laptop (or other PC), 2018. Online: <http://mininet.org/>.