SUBJECT:

Study on the behavior of third-generation neural network models in preventing DDoS attacks

SUPERVISOR:

dr hab. inż. Grzegorz Borowik
grzegorz.borowik@nask.pl
NASK-PIB, Centrum Badań i Rozwoju
Kolska 12, 01-045 Warszawa

DESCRIPTION:

The aim of this thesis is to study the behavior of different neural network models, including third-generation models (Spiking Neural Networks), in preventing DDoS attacks. Various neural network architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) will be analyzed to understand the factors that influence their effectiveness in detecting and preventing DDoS attacks. Subsequently, the results of these works will be compared with the behavior analysis of Spiking Neural Networks in preventing DDoS attacks.

The research will be based on a dataset that includes different types of DDoS attacks. Many experiments and tests will be conducted to evaluate the effectiveness of each model in different conditions and scenarios. The computational and memory complexities of each model will also be analyzed to understand their performance in practical applications.

In this thesis, new machine learning methods will also be proposed, such as transfer learning techniques and hybrid neural network models. The goal is to increase the effectiveness and efficiency of models in preventing DDoS attacks. Ultimately, this work will contribute to the development of the cybersecurity field and help in the development of more effective methods to counter DDoS attacks.

BIBLIOGRAPHY:

1. Jyothi, V., Wang, X., Addepalli, S., & Karri, R. (2016). BRAIN: BehavioR Based Adaptive Intrusion Detection in Networks: Using Hardware Performance Counters to Detect DDoS Attacks. 2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), 587-588.
2. Yuan, X., Li, C., & Li, X. (2017). DeepDefense: Identifying DDoS Attack via Deep Learning. 2017 IEEE International Conference on Smart Computing (SMARTCOMP), 1-8.
3. Ye, J., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). A DDoS Attack Detection Method Based on SVM in Software Defined Network. Secur. Commun. Networks, 2018, 9804061:1-9804061:8.
4. Peraković, D., Periša, M., Cvitić, I., & Husnjak, S. (2016). Artificial neuron network implementation in detection and classification of DDoS traffic. 2016 24th Telecommunications Forum (TELFOR), 1-4.

5. Elsayed, M.S., Le-Khac, N., Dev, S., & Jurcut, A.D. (2020). DDoSNet: A Deep-Learning Model for Detecting Network Attacks. 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 391-396.
6. Li, J., Liu, Y., & Gu, L. (2010). DDoS attack detection based on neural network. 2010 2nd International Symposium on Aware Computing, 196-199.
7. Izhikevich, E.M. (2003). Simple model of spiking neurons. IEEE transactions on neural networks, 14 6, 1569-72.
8. Huh, D., & Sejnowski, T.J. (2017). Gradient Descent for Spiking Neural Networks. Neural Information Processing Systems.