A Cost-based Approach for Fast Intrusion Detection

Jiarui Gao[1]
[1]School of Computer Science, Shanghai Key Laboratory of Intelligent Information Processing,
Fudan University, China
jrgao14@fudan.edu.cn

ABSTRACT

The aim of Intrusion Detection System(IDS) is to maximize detection accuracy as well as minimize corresponding costs. In this paper, I present a cost-based approach utilizing neural network with GPU acceleration for fast intrusion detection. In this approach, both computational cost and feature cost are considered, and models are trained with respect to their different protocol types and services. Empirical experiments are carried out on off-line benchmark dataset NSL-KDD.

KEYWORDS

Neural network; Intrusion detection; anomaly detection; cost analysis.

ACM Reference format:
Jiarui Gao[1]. 2017. A Cost-based Approach for Fast Intrusion Detection . In *Proceedings of* , , , 1 pages.
DOI: http://dx.doi.org/xxx

1 INTRODUCTION

With the development of computing and Internet technology, Internet has became an important part of our daily life. However, this popularity has also brought security issues. Intrusion Detection Systems(IDSs) are designed to detect attacks, which help discover, determine, and identify unauthorized use, duplication, alteration, and destruction of information systems[4]. Specifically, IDSs are able to monitor intrusions and alert network administrators if necessary.

According to the detectable attacks, there are mainly three types of IDSs: misuse-based, anomaly-based, and hybrid[1]. Misuse-based IDSs are designed to detect known attacks by comparing signatures of those attacks and those in the database. Anomaly-based IDSs have the ability for detecting zero-day attacks. The normal network are modeled and anomalies can be detected when happened.

Also with respect for using environment, IDSs can be used in real-time environment of off-line environment. Off-line IDSs have been studied extensively recently. However, these systems fail to provide real time information, which means they can only detect intrusions after they already happened. The challenge for real-time IDSs is the huge cost brought with the detection.

In this paper, the aim is to develop a IDS which can be utilized in real-time environment with high detection accuracy. I present a cost-based approach for anomaly intrusion detection. The traditional machine learning models are replaced by neural networks, which enable the computational cost to be minimized utilizing GPU acceleration. Also, the feature cost is considered, and according to the feature cost theory in [3], low level features are utilized with high priority. The benchmark dataset NSL-KDD is used for evaluation, which is a new version of dataset KDDCUP'99[2] and has significant improvements compared with KDDcup99[5].

The rest of the paper is organized as follows.

2 RELATED WORK

3 METHODOLOGY

4 EXPERIMENTS

5 CONCLUSION

REFERENCES

[1] Anna L Buczak and Erhan Guven. 2016. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials* 18, 2 (2016), 1153–1176.

[2] KDD Cup. 2007. Available on: http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html. (2007).

[3] Wenke Lee, Salvatore J Stolfo, Philip K Chan, Eleazar Eskin, Wei Fan, Matthew Miller, Shlomo Hershkop, and Junxin Zhang. 2001. Real time data mining-based intrusion detection. In *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings*, Vol. 1. IEEE, 89–100.

[4] Srinivas Mukkamala, Andrew Sung, and Ajith Abraham. 2005. Cyber security challenges: Designing efficient intrusion detection systems and antivirus tools. *Vemuri, V. Rao, Enhancing Computer Security with Smart Technology.(Auerbach, 2006)* (2005), 125–163.

[5] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. 2009. A detailed analysis of the KDD CUP 99 data set. In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*. IEEE, 1–6.

,

© 2017 ACM. ACM ISBN xxx…$15.00
DOI: http://dx.doi.org/xxx