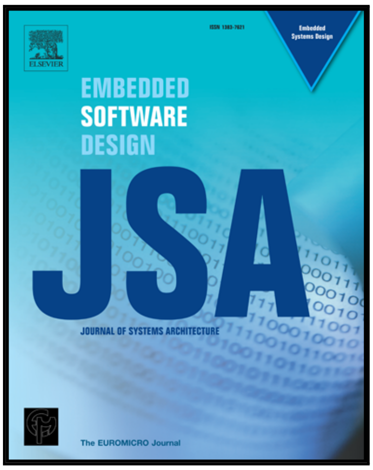

# Multi-Task Learning for Intrusion Detection on Web Logs

Bo Li, Ying Lin, Simin Zhang

PII: S1383-7621(17)30299-0
DOI: 10.1016/j.sysarc.2017.10.011
Reference: SYSARC 1470

To appear in: *Journal of Systems Architecture*

Received date: 29 June 2017
Revised date: 19 September 2017
Accepted date: 16 October 2017

Please cite this article as: Bo Li, Ying Lin, Simin Zhang, Multi-Task Learning for Intrusion Detection on Web Logs, *Journal of Systems Architecture* (2017), doi: 10.1016/j.sysarc.2017.10.011

# Multi-Task Learning for Intrusion Detection on Web Logs

Bo Li[a], Ying Lin[a], Simin Zhang[a,*]

[a] *School of Computer Science and Engineering, Beihang University, Beijing 100191, China*

## Abstract

In this paper, we aim to detect malicious network activities based on the analysis of web logs. Despite recent advances, classifying all malicious activities into specific types as well as identifying novel attacks are still serious issues. Various kinds of attacks have different representations. In traditional approaches, detecting each kind of attack is usually considered as an independent task. However, it is observed that different types share some common features in URL, which can be formulated as a multi-task problem. Inspired by this observation, we propose a novel Multi-Task Learning Intrusion Detection (MTLID) approach to share these common features across all types, which improves the performance of classification. Moreover, in order to detect the false negatives introduced by multi-task classification, we adopt Gaussian Mixture Model (GMM) to build the profile of normal activities, and thereby novel attacks could be further identified. We obtain a real-world dataset of web logs from different websites to demonstrate the effectiveness of MTLID. Experiment results illustrate that our proposed approach outperforms existing methods in both detection rate and false alarm rate.

*Keywords:* Intrusion Detection; Multi-Task Learning; Web Logs; Gaussian Mixture Model (GMM).

[*] Corresponding author

*Email addresses:* libo@act.buaa.edu.cn (Bo Li), linying@act.buaa.edu.cn (Ying Lin), zhangsm14@act.buaa.edu.cn (Simin Zhang)