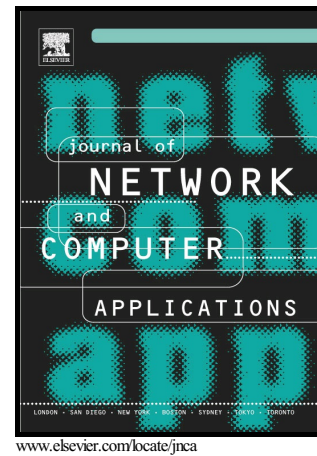


# Author's Accepted Manuscript

Model Order Selection and Eigen Similarity based Framework for Detection and Identification of Network Attacks

Thiago P.B. Vieira, Danilo F. Tenório, João Paulo C.L. da Costa, Edison P. de Freitas, Giovanni Del Galdo, Rafael T. de Sousa Júnior



PII: S1084-8045(17)30160-1  
DOI: <http://dx.doi.org/10.1016/j.jnca.2017.04.012>  
Reference: YJNCA1909

To appear in: *Journal of Network and Computer Applications*

Received date: 31 May 2016  
Revised date: 4 January 2017  
Accepted date: 19 April 2017

Cite this article as: Thiago P.B. Vieira, Danilo F. Tenório, João Paulo C.L. da Costa, Edison P. de Freitas, Giovanni Del Galdo and Rafael T. de Sousa Júnior, Model Order Selection and Eigen Similarity based Framework for Detection and Identification of Network Attacks, *Journal of Network and Computer Applications*, <http://dx.doi.org/10.1016/j.jnca.2017.04.012>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting galley proof before it is published in its final citable form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain

# Model Order Selection and Eigen Similarity based Framework for Detection and Identification of Network Attacks

Thiago P. B. Vieira<sup>a</sup>, Danilo F. Tenório<sup>a</sup>, João Paulo C. L. da Costa<sup>a,b,c</sup>, Edison P. de Freitas<sup>d</sup>, Giovanni Del Galdo<sup>b,c</sup>, Rafael T. de Sousa Júnior<sup>a</sup>

<sup>a</sup>*Department of Electrical Engineering, University of Brasilia (UnB), 70910-900, Brasília-DF, Brazil*

<sup>b</sup>*Institute for Information Technology, Ilmenau University of Technology, Ilmenau, Germany*

<sup>c</sup>*Fraunhofer Institute for Integrated Circuits IIS, Erlangen, Germany*

<sup>d</sup>*Graduate Program in Electrical Engineering, Federal University of Rio Grande do Sul (UFRGS), 90035-190, Porto Alegre, Brazil*

---

## Abstract

Novel schemes for attack detection are crucial to identify adaptive malicious traffic coming from sources that are quickly mobilized by attackers in high throughput communication networks. In this context, signal processing techniques have been applied to attack detection due to their capability to detect anomalies that are previously unknown, i.e. blind detection. This paper proposes a signal processing framework for the detection and identification of network attacks using concepts of model order selection (MOS), eigenvalues and similarity analysis. In order to validate the proposed framework, we consider network traffic datasets that contain malicious activity such as flood and port probing attacks. We propose to model the network traffic as a superposition of components, namely, user's operations (legitimate traffic), network service operation not related to the user (noise) and the malicious activity. The experiments performed in a real network and also using the DARPA 1998 public dataset show that the proposed blind detection approach achieves satisfactory levels of accuracy in terms of timely detection and identification of TCP/UDP ports under attack.

*Keywords:* Network Attack Detection, Model Order Selection, Eigen Analysis, Similarity Analysis

---

Download English Version:

<https://daneshyari.com/en/article/4955892>

Download Persian Version:

<https://daneshyari.com/article/4955892>

[Daneshyari.com](https://daneshyari.com)