Accepted Manuscript

A novel statistical technique for intrusion detection systems

Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuo

PII: S0167-739X(17)30137-1
DOI: http://dx.doi.org/10.1016/j.future.2017.01.029
Reference: FUTURE 3311

To appear in: *Future Generation Computer Systems*

Received date: 8 August 2016
Revised date: 16 December 2016
Accepted date: 22 January 2017

Please cite this article as: E. Kabir, J. Hu, H. Wang, G. Zhuo, A novel statistical technique for intrusion detection systems, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.01.029

A Novel Statistical Technique for Intrusion Detection Systems

Enamul Kabir, Jiankun Hu, and Hua Wang, and Guangping Zhuo*†‡§

Abstract

This paper proposes a novel approach for intrusion detection system based on sampling with Least Square Support Vector Machine (LS-SVM). Decision making is performed in two stages. In the first stage, the whole dataset is divided into some predetermined arbitrary subgroups. The proposed algorithm selects representative samples from these subgroups such that the samples reflect the entire dataset. An optimum allocation scheme is developed based on the variability of the observations within the subgroups. In the second stage, least square support vector machine (LS-SVM) is applied to the extracted samples to detect intrusions. We call the proposed algorithm as optimum allocation-based least square support vector machine (OA-LS-SVM) for IDS. To demonstrate the effectiveness of the proposed method, the experiments are carried out on KDD 99 database which is considered a de facto benchmark for evaluating the performance of intrusions detection algorithm. All binary-classes and multiclass are tested and our proposed approach obtains a realistic performance in terms of accuracy and efficiency. Finally a way out is also shown the usability of the proposed algorithm for incremental datasets.

keywords: Sampling, Intrusion Detection System (IDS), Network Security, Least Square Support Vector Machine (LS-SVM).

1 Introduction

In recent years, there has been an increasing awareness of the risk associated with network attacks as information systems are now more open to the Internet than ever before. Intrusion detection system (IDS) is a program that tries to find indications that the computer has been compromised. An IDS attempts to detect an intruder breaking into computer system or legitimate user misuses system resources. Intrusion detection is an important issue and has captured the attention of network administrators and security professionals.

Intrusion detection is the art of detecting unauthorized, inappropriate, or anomalous activity on computer systems. Intrusion detection systems are classified as network based,

*Enamul Kabir is with the School of Agricultural, Computational and Environmental Sciences, University of Southern Queensland, Toowoomba, QLD 4350, Australia. E-mail: Enamul.Kabir@usq.edu.au

†Jiankun Hu is with the School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra, ACT 2600,Australia. E-mail: J.Hu@adfa.edu.au

‡Hua Wang is with Centre for Applied Informatics, Victoria University, Melbourne, VIC 8001, Australia/Department of Computer Science,Taiyuan Normal University, China. E-mail: Hua.Wang@vu.edu.au

§Guangping Zhuo is with Department of Computer Science, Taiyuan Normal University, China. E-mail: zhuoguangping@163.com