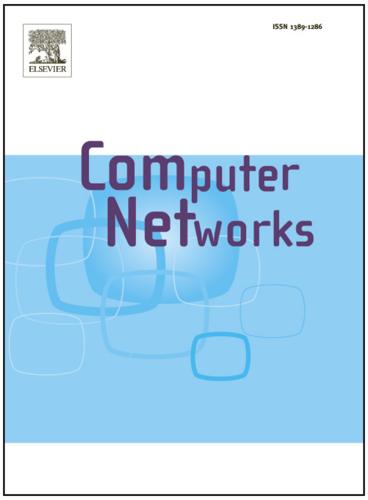

Towards Adaptive Character Frequency-based Exclusive Signature Matching Scheme and its Applications in Distributed Intrusion Detection

Yuxin Meng, Wenjuan Li, Lam-for Kwok

PII: S1389-1286(13)00265-X
DOI: http://dx.doi.org/10.1016/j.comnet.2013.08.009
Reference: COMPNW 5076

To appear in: *Computer Networks*

Received Date: 26 March 2013
Accepted Date: 8 August 2013

Please cite this article as: Y. Meng, W. Li, L-f. Kwok, Towards Adaptive Character Frequency-based Exclusive Signature Matching Scheme and its Applications in Distributed Intrusion Detection, *Computer Networks* (2013), doi: http://dx.doi.org/10.1016/j.comnet.2013.08.009

Towards Adaptive Character Frequency-based Exclusive Signature Matching Scheme and its Applications in Distributed Intrusion Detection☆

Yuxin Meng[a], Wenjuan Li[b], Lam-for Kwok[a]

E-mail address: ymeng8@student.cityu.edu.hk, cslfkwok@cityu.edu.hk

*[a]Department of Computer Science,
City University of Hong Kong, Hong Kong SAR, China
[b]Computer Science Division,
Zhaoqing Foreign Language College, Guangdong, China*

Abstract

Network intrusion detection systems (NIDSs), especially signature-based NIDSs, are being widely deployed in a distributed network environment with the purpose of defending against a variety of network attacks. However, signature matching is a key limiting factor to limit and lower the performance of a signature-based NIDS in a large-scale network environment, in which the cost is at least linear to the size of an input string. The overhead network packets can greatly reduce the effectiveness of such detection systems and heavily consume computer resources. To mitigate this issue, a more efficient signature matching algorithm is desirable. In this paper, we therefore develop an adaptive character frequency-based exclusive signature matching scheme (named *ACF-EX*) that can improve the process of signature matching for a signature-based NIDS. In the experiment, we implemented the *ACF-EX* scheme in a distributed network environment, evaluated it by comparing with the performance of Snort. In addition, we further apply this scheme to constructing a packet filter that can filter out network packets by conducting exclusive signature matching for a signature-based NIDS, which can avoid implementation issues and improve the flexibility of the scheme. The experimental results demonstrate that, in the distributed network environment, the proposed *ACF-EX* scheme can positively reduce the time consumption of signature matching and that our scheme is promising in constructing a packet filter to reduce the burden of a signature-based NIDS.

Keywords:
Network Intrusion detection, Exclusive Signature Matching, Distributed Systems, Packet Filter, Network Security and Performance.

1. Introduction

Network intrusions (e.g., malware, exploits) are becoming a critical issue for the whole network communications [3]. To mitigate this issue, network intrusion detection systems (NIDSs) [4, 5] have been widely implemented in different network environments, aiming to enhance network security by defending against different kinds of network attacks. In addition, these intrusion detection systems have already deployed in a distributed environment (e.g., agent-based network, mobile ad hoc network-MANET) to perform detection of intrusions.

Roughly, network intrusion detection systems can be categorized into two folders: *signature-based NIDS* and *anomaly-based NIDS*. A signature-based NIDS [7, 6] (also called *rule-based NIDS* or *misuse-based NIDS*) detects an attack by comparing its signatures with incoming packet payloads. A *signature* (also called *rules*) can be regarded as a kind of descriptions for a known attack. On the other hand, an anomaly-based NIDS [9, 11] identifies an attack by discovering significant deviations between its pre-established *normal profile*[1] and current observed network events. Based on the detection modes, the anomaly-based NIDS has the capability of discovering novel network attacks. However, it is very

☆A preliminary version of this paper appears in Proc. of Int'l Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom 2012) [1] and Int'l Conf. on Computer and Information Science (ICIS 2012) [2].

[1] A *normal profile* is used to present the normal behavior of a user or network connection.