An Enhanced Fuzzy ARM Approach for Intrusion Detection

Nasser S. Abouzakhar, The University of Hertfordshire, UK
Huankai Chen, The University of Hertfordshire, UK
Bruce Christianson, The University of Hertfordshire, UK

ABSTRACT

The integration of fuzzy logic with data mining methods such as association rules has achieved interesting results in various digital forensics applications. As a data mining technique, the association rule mining (ARM) algorithm uses ranges to convert any quantitative features into categorical ones. Such features lead to the sudden boundary problem, which can be smoothed by incorporating fuzzy logic so as to develop interesting patterns for intrusion detection. This paper introduces a Fuzzy ARM-based intrusion detection model that is tested on the CAIDA 2007 backscatter network traffic dataset. Moreover, the authors present an improved algorithm named Matrix Fuzzy ARM algorithm for mining fuzzy association rules. The experiments and results that are presented in this paper demonstrate the effectiveness of integrating fuzzy logic with association rule mining in intrusion detection. The performance of the developed detection model is improved by using this integrated approach and improved algorithm.

Keywords: Algorithms, Cybercrime Detection, Forensic Computing, Intrusion Detection, Matrix Fuzzy ARM

INTRODUCTION

The wide spread use of the Internet and WWW in today’s society led to various security vulnerabilities and threats. Such security problems have become increasingly important and an international priority to many organizations and countries. Within the network security community, researching network intrusion and current attacks is one of the major challenges, particularly, researching denial-of-service attacks. Intrusion detection (Proctor, 2001) is the process of monitoring computer and/or network activities and events, analysing them for signs of security threats such as unauthorised access, malicious activities and violations for security policy. Intrusion Detection Systems (IDSs) are capable of observing patterns of activities in user accounts and detect malicious behaviour. Intrusion detection systems are usually divided into two types (Carter, 2002): misuse detection approach and anomaly detection approach. The misuse detection approach tends to look for events that match certain network behaviors against well-defined intrusive patterns that are precisely written in advance. The anomaly detection approach attempts to evaluate a user

DOI: 10.4018/jdcf.2011040104
or system behavior and consider intrusive or irregular activities as some deviation from the normal patterns. Such approach is capable of identifying newly developed attacks for which a well-defined intrusive pattern does not exist.

Denial-of-service (DoS) attack (Moore et al., 2006; Tague, et al., 2009) is a computer network-based attack where an attacker floods a computer system or a network (victim) with useless traffic. Such attacks are difficult to be avoided since it is hard to distinguish the “good” requests from the “bad” ones. The association rule mining (ARM) technique (Agrawal & Srikant, 1994) has been applied into anomaly detection to automatically mine abnormal patterns from network data and/or audit data. One of the major limitations of such a mining approach (Changguo et al., 2009; Bridges, et al., 2000) of dealing with quantitative features is the sudden boundary problem. For example, an intrusion that deviates only slightly from the normal acceptable patterns may not be detected or a small change in normal patterns may trigger a false alarm. In order to deal with such a problem and improve the flexibility of the system, fuzzy logic has been integrated with ARM technique for intrusion detection.

It is possible to integrate fuzzy logic (Luo, 1999) with ARM as many quantitative features that are involved in intrusion detection can be treated as fuzzy variables. An example of quantitative feature is the number of different SYN flags in a fixed-interval of 1 sec or 2 sec. In traditional association rule mining, given a quantitative boundary, the quantitative feature can be split into two levels of categories i.e. Low or High. Any values of the quantitative feature falling below the boundary will be categorised as Low. Those values falling above the boundary will be categorised as High. Regardless of their distance to the boundary all values are categorised as either Low or High. Such an approach leads to the sudden separation of Low and High, which can be smoothed by integrating the Fuzzy Logic.

We present a new FARM algorithm named Matrix Fuzzy Association Rule Mining (Matrix FARM) algorithm. This algorithm improves the performance of the proposed detection model which uses FARM techniques to mine new patterns from the network traffic dataset. The model calculates the similarity between the new patterns and the normal patterns mined from normal network traffic. If the similarity value is under a user-defined threshold, the model will generate an alarm indicate that there may be some anomalies occurred in the network traffic. The evaluation of the proposed new model is achieved by testing the performance of the developed Matrix FARM using standard methods.

**RELATED WORK**

Fuzzy association rule mining (FARM) intrusion detection model (Florez et al., 2002) combines techniques from association rule mining and fuzzy logic. Association rule mining is used to automatically learn various patterns and events from large quantities of network traffic dataset. In standard ARM, quantitative values are converted to be either completely a member of a particular group/category or not a member at all. However, fuzzy logic technique enables quantitative values to be represented in more than one category. This means that a quantitative value can be a partial member in one category while possibly being a member of another category. The integration of fuzzy logic with association rule mining allows the development of more flexible patterns for intrusion detection.

**ARM Intrusion Detection**

As a supervised learning technique (Sánchez et al., 2009; Su et al., 2009), the data mining technique association rule mining (ARM) can be trained to mine normal patterns from training data. We introduce an ARM algorithm for mining flexible patterns and develop fast model, which respectively could improve the accuracy and efficiency of the intrusion detection. Association rules are capable of representing correlations between a set of attribute values in the dataset. Agrawal and Srikant (1994) have
Related Content

U.S. Federal Data Mining Programs in the Context of the War on Terror: The Congress, Court, and Concerns for Privacy Protection
www.igi-global.com/chapter/federal-data-mining-programs-context/60990?camid=4v1a

On More Paradigms of Steganalysis
www.igi-global.com/article/on-more-paradigms-of-steganalysis/150855?camid=4v1a

Trust Management in Mobile Ad Hoc Networks for QoS Enhancing
www.igi-global.com/chapter/trust-management-in-mobile-ad-hoc-networks-for-qos-enhancing/131401?camid=4v1a
Forensic Readiness and eDiscovery
www.igi-global.com/chapter/forensic-readiness-and-ediscovery/115757?camid=4v1a