


Network Anomalies Detection Approach Based on Weighted Voting

Sergey Sakulin, Bauman Moscow State Technical University, Russia


 <https://orcid.org/0000-0001-9218-9725>

Alexander Alfimtsev, Bauman Moscow State Technical University, Russia*


 <https://orcid.org/0000-0002-3805-4499>

Konstantin Kvitchenko, Moscow Credit Bank, Russia

Leonid Dobkacz, Bauman Moscow State Technical University, Russia

 <https://orcid.org/0000-0001-6455-8650>

Yuri Kalgin, Bauman Moscow State Technical University, Russia

 <https://orcid.org/0000-0003-0091-1579>

Igor Lychkov, Bauman Moscow State Technical University, Russia

ABSTRACT

To avoid information systems malfunction, their integrity disruption, availability violation, as well as data confidentiality, it is necessary to detect anomalies in information system operation as quickly as possible. The anomalies are usually caused by malicious activity – information systems attacks. However, the current approaches to detect anomalies in information systems functioning have never been perfect. In particular, statistical and signature-based techniques do not allow detection of anomalies based on modifications of well-known attacks. Dynamic approaches based on machine learning techniques result in false responses and frequent anomaly miss-outs. Therefore, various hybrid solutions are being frequently offered on the basis of those two approaches. The paper suggests a hybrid approach to detect anomalies by combining computationally efficient classifiers of machine learning with accuracy increase due to weighted voting. Pilot evaluation of the developed approach proved its feasibility for anomaly detection systems.

KEYWORDS

CICIDS2017 Dataset, Classifier Ensembles, Machine Learning, Network Anomaly Detection, Signature-Based Technique

1. INTRODUCTION

It is highly important to quickly detect anomalies in complex computer networks, the ones that can be caused by malicious attacks. Such attacks can result in network inability to function properly, data loss or misrepresentation or even its leak. For early detection of anomalies special software systems are used to detect and classify them. Similar systems are built on the basis of the traditional signature-

DOI: 10.4018/IJISP.2022010105

*Corresponding Author

based techniques to detect anomalies (Afek et al., 2019; AlYousef & Abdelmajeed, 2019), as well as machine learning techniques (Sultana et al., 2019; Yu et al., 2017). Signature-based techniques do not allow detection of anomalies caused by attacks that are some modifications of well-known attacks (Chakravarty et al., 2019), and approaches based on machine learning can result in false responses and anomaly miss-outs (Gao et al., 2019; Umer et al., 2017).

Many specialists have been working to overcome these drawbacks (Xu et al., 2018; Raman et al., 2017; Le et al., 2017). In particular, the signatures are used as a training set to train classifiers (Hoang & Nguyen, 2019). There are hybrid approaches based on ensembles of classifiers (Khraisat et al., 2019; Zhang et al., 2018). The existing approaches however do not allow detection of anomalies that are relevant to new or formally known modified attacks with high accuracy and low number of false positive responses at the same time.

In these conditions the search for more reliable approaches to detect anomalies has become urgent. The paper offers a hybrid approach to detect anomalies by signature analysis and weighted voting of classifiers that are built on the basis of machine learning. The classifiers were chosen to be logistic regression, stochastic gradient descent and decision tree. Such a choice is explained by relatively low computational complexity of algorithms, because the anomaly detection system is designed to operate in real time. The experiments carried out proved that the suggested approach features high accuracy of detection of well-known and new anomalies as well as high repetitiveness.

Further, the paper is organized as follows: **section 2** considers some studies about anomaly detection where we will choose suitable components to implement the combined approach as well as view various datasets and choose a suitable to investigate the suggested approach; **section 3** describes the suggested approach; **section 4** fully considers the experiment carried out and draws the conclusion about the effectiveness of the suggested approach and the potential of the research in this field.

2. RELATED WORKS

2.1. Approaches to Detect Anomalies

There have been various classifications of approaches to detect network anomalies. In particular, in study (Ahmed et al., 2016) the approaches are divided into the following groups:

- Knowledge-based techniques (where signature analysis is most frequently used);
- Behavioral techniques;
- Statistical techniques;
- Classifiers based on machine learning and data mining (which include decision trees, logistic regression, support vector machine, artificial neural networks and many others);
- Ensembles of several classifiers and hybrid approaches.

Each of the approaches to detect anomalies has its advantages and disadvantages. In particular, signature analysis is almost faultless for the first and second types of errors when detecting well-known anomalies. Computational complexity depends on the size of signature base and the number of parameters of each signature.

Behavioral and statistical techniques feature the problems with accuracy and low prevalence (Ahmed et al., 2016). That is why we do not consider them in our study.

Hybrid approaches together with signature analysis employ ensembles of classifiers based on machine learning. These ensembles are implemented by the terminal classifier which irreversibly relegates the current event of network activity to a certain group by aggregating classifiers outputs (Choi & Jang, 2018). Such approaches allow us to receive higher accuracy and detect both well-known and unknown anomalies (Fernandes et al., 2019). Some classifiers are limited to be used in hybrid approaches because of their computational complexity.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/network-anomalies-detection-approach-based-on-weighted-voting/284050

Related Content

A Systematic Study and Analysis of Security Issues in Mobile Ad-hoc Networks

Jhum Swain, Binod Kumar Pattanayak and Bibudhendu Pati (2018). *International Journal of Information Security and Privacy* (pp. 38-45).

www.irma-international.org/article/a-systematic-study-and-analysis-of-security-issues-in-mobile-ad-hoc-networks/201509

A Proposed Scheme for Remedy of Man-In-The-Middle Attack on Certificate Authority

Sarvesh Tanwar and Anil Kumar (2017). *International Journal of Information Security and Privacy* (pp. 1-14).

www.irma-international.org/article/a-proposed-scheme-for-remedy-of-man-in-the-middle-attack-on-certificate-authority/181544

Real-Time Cyber Analytics Data Collection Framework

Herbert Maosa, Karim Ouazzane and Viktor Sowinski-Mydlarz (2022). *International Journal of Information Security and Privacy* (pp. 1-10).

www.irma-international.org/article/real-time-cyber-analytics-data-collection-framework/311465

An Improved Separable and Reversible Steganography in Encrypted Grayscale Images

Manisha Duevedi and Sunil Kumar Muttu (2021). *International Journal of Information Security and Privacy* (pp. 1-28).

www.irma-international.org/article/an-improved-separable-and-reversible-steganography-in-encrypted-grayscale-images/276382

An Adaptive Threat-Vulnerability Model and the Economics of Protection

C. Warren Axelrod (2009). *Social and Human Elements of Information Security: Emerging Trends and Countermeasures* (pp. 262-282).

www.irma-international.org/chapter/adaptive-threat-vulnerability-model-economics/29056