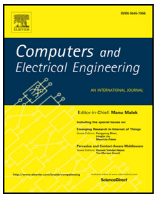
Computers and Electrical Engineering 000 (2017) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng



A novel network security algorithm based on improved support vector machine from smart city perspective[☆]

Xiang Zou[a], Jinghua Cao[b,*], Quan Guo[c], Tao Wen[a]

[a] Northeastern University, Liaoning, China
[b] Dalian Maritime University, Liaoning, China
[c] Provincial Key Laboratory, Dalian Neusoft University of Information, China

ARTICLE INFO

Article history:
Received 11 December 2016
Revised 22 September 2017
Accepted 25 September 2017
Available online xxx

Keywords:
Data mining
Intrusion detection system/intrusion prevention system
One class-support vector machine
Decision tree learning-iterative dichotomise 3

ABSTRACT

Computer generated security concerns have become more modern and complex. Intrusion detection(ID) is a practical issue in the field of computer security whose primary objective is to detect rare attack or assaults and to ensure the security of interior systems. This paper also proposes a semi-class intrusion detection method that combines multiple classifiers to arrange exceptions and typical exercises in a computer system. The abuse detection model is constructed in the light of the decision tree learning-iterative dichotomise 3(DTL-ID3) and is assembled by utilizing the gathered data based on anomaly detection model executed by one class-support vector machine(OC-SVM). In recent years, people have paid more attention to ID/intrusion prevention system (IDS / IPS), which is closely related to the protection and utilization of system management. A few machine-learning standards including neural system, direct hereditary programming, and advanced support vector machines(ASVMs), Bayesian system, multivariate versatile relapse splines, fluffy derivation systems(FIS) and other analogical systems have been researched for the outline of intrusion detection system. In this paper, we build up an amalgam method based on DTL-ID3 and OC-SVM(A-DT and SVM) and evaluate the performance of the projected methodology by using a specific dataset and a crossover method in order to enhance the accuracy of IDS/IPS when contrasted with a singular support vector machine.

1. Introduction

The fast advancement and improvement of the Internet has brought security problems to systems which is progressively becoming a extraordinary issue and has been a concentration in the ebb and flow exploration. In recent years, people pay more attention to the problem of IDS, which is closely related to the covert use of system management [3]. In any case, it is difficult to detect the assault and the typical system access. In today's IDS, large-scale information grouping and scheduling has become increasingly important and has become a test area. Albeit different apparatuses are projected, they are productive for certain applications adequately, which are used for exponential developing high dimensional information inputs [7,9]. Intrusion detection systems are designed to protect computer systems from various digital attacks and infections [13]. The intrusion detection system constructs a robust feature model and examples to identify the general practices of system information described by nonstandard practices. Two basic hypotheses in intrusion detection are studied, for example, client

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. S. Smys.

[*] Corresponding author at: Software Center, Northeastern University, No. 3-11, Wenhua Road, Heping District, Liaoning, China.
E-mail address: zouxiangman123@sina.com (J. Cao).

https://doi.org/10.1016/j.compeleceng.2017.09.028
0045-7906/© 2017 Published by Elsevier Ltd.

and program exercises can be recognized by PC systems according to system reviewing mechanisms, and ordinary and intrusion exercises must have particular practices. The field of intrusion detection consists of two different approaches, that are abuse detection and anomaly detection [17,18]. The basic idea of misuse of investigation is to detect the attack of a certain type or target in some way, and even identify the types of these attacks. In view of these signs, this method identifies attacks by describing the criteria for each known attack [1]. The trouble for identifying obscure assaults has become a fundamental drawback in the mark-based method. The primary objective of the anomaly detection method is to describe the typical activities of the manufacturing factual model. In this point, any deviation from this model can be viewed as an anomaly, and perceived as an assault [20]. When this approach is utilized, it can identify obscure assaults hypothetically, despite the fact happened now and again, the considered approach gives rise to high false assault rate. Given the general manufacture models in the past few years, people are keen to develop new manufacturing models [6,10].

Anomaly detection approach is one of the extremely dynamic researches in the machine learning group, which has been the theme of presented numerous articles over many years. The best approach depends on gathering information from typical operations of the system. In view of this information portraying ordinariness, if any deviation is seen in any case, it would be considered as an anomaly [11]. A few machine learning standards include the hidden Markov model, bolster VM, fake neural system, counterfeit neural system and multivariate versatile relapse splines fluffy surmising systems, which have been researched for the outline of IDS [19]. In the manuscript, we conduct researches and assess the performance of OC-SVM. The proposed amalgam method based on decision tree learning-ID3 and OC-SVM is a combination of A-DT and SVM. Compared with the different methods, it can improve the accuracy of IDS intrusion detection system by using half method [27]. The rest of the paper is organized as the follows. In the Section 2, we review the state-of-the-art related works; in the Section 3, we introduced IEEE Transactions on Reliability; in the Section 4, we discussed the DTL-ID3; in the Section 5, we analysed the A-DT & SVM; in the Section 6, we implemented the proposed method with the experimental simulation; the Section 7 summarized the work.

2. Related works

Unique strategies and methods are used as part of future development. The primary procedures utilized in this paper are measurable methodologies, prescient example era, master systems, keystroke observing, demonstrate based state transition analysis, intrusion detection, design coordinating, and information mining strategies. The fact methodology examines the late behaviour of PC system clients. Remarkably, abnormal behaviour is considered an invasion [2]. The method needs to improve the behaviour model of the general customer behaviour. This infringement occurs when customer behaviour deviates from normal behaviour. IDS abuses the factual methodology for detection of interlopers [4]. A specialist system takes up an issue space to arrange the principles. The standards include all parts, antecedent features are linked and followed which characterizes actions that should be taken into account in the event of prior performance. Manage is released when example coordinating systems establishes that watched monitoring information to coordinate or satisfy the antecedent of the operation [5,8]. The guidelines can be aware of the single audit situation, saying there is no input to the major risks of the system, or they may perceive a succession of occasions that speak to a whole entrance situation. There are a few drawbacks with master system method. Intrusion situation does not trigger administer that cannot be recognized based on the running based method [12]. Keeping up and redesigning an intricate govern based system might lead to trouble [14].

Model-based (MB) approach endeavours ideal intrusions are dedicated to reflection rather than review track proceedings [15]. The main purpose of this study is to establish a context model to reveal the trademark behaviour of the invasion. The upper section allows dynamic creation of the representation of penetration, which changes weights to calculate the putative inheritance record of the master solution [16]. This program is different from the current lead based system strategy, which basically endeavours to example coordinate review records to master rules. Broad researches have been done for detection of half breed intrusion detection and highlight determination [23]. Another hybrid intrusion detection method is gradually shown as misuse detection and anomaly detection in the decay structure. Abuse detection model is assembled in view of DTL-ID3 and is utilized to disintegrate the typical preparing information into littler subsets, and OC-SVM is utilized to make anomaly-detection for the deteriorated area. DTL-ID3 does not frame a bunch, conversely it can debase the profiling capacity.

In view of squid enhancement computation in intrusion detection system, we propose a new element selection method. The cuttlefish calculation (CFA) is used in the model which is utilized to discover ideal subset of components and ID3 classifier regarded as a judgment tool on the choice highlights that are delivered by the cuttlefish calculation [25,26]. A cuttlefish algorithm is recommended that was a novel bio-inspired optimization algorithm. Another meta-heuristic bio-propelled advancement calculation, cuttlefish algorithm is introduced. This method accomplishes better performance in contrast with genetic algorithm (GA), PSO, ant colony optimization (ACO). An anomaly detection method utilizing K-means alongside decision tree learning-ID3, technique to along K-means bunching forward and the DTL-ID3 methods. This method accomplishes better performance in contrast with K-means, iterative dichotomise 3 and one class-SVM. An anomaly activity detection system was anticipated in the light of the entropy of system components and OC-SVM, then cross breed method is a mix of both entropy and one class-SVM (OC-SVM) which is a contrasted and individual method. Amalgam is consistent with a single method of precision, but it does not dynamically select whether there is an attack and leads to high false positives. Another approach was anticipated, in view of artificial neural network and fluffy grouping, to deal with the issues in the intrusion detection system. Compared with back propagation, the proposed method has better detection accuracy and detection intensity.

Please cite this article as: X. Zou et al., A novel network security algorithm based on improved support vector machine from smart city perspective, Computers and Electrical Engineering (2017), https://doi.org/10.1016/j.compeleceng.2017.09.028