Pattern Recognition Letters 85 (2017) 56–64

Contents lists available at ScienceDirect

Pattern Recognition Letters

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

Real-time multi-agent system for an adaptive intrusion detection system

Wathiq Laftah Al-Yaseen[a,b,*], Zulaiha Ali Othman[a], Mohd Zakree Ahmad Nazri[a]

[a] Data Mining and Optimization Research Group (DMO), Centre for Artificial Intelligence Technology (CAIT), School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 Bandar Baru Bangi, Malaysia
[b] Al-Furat Al-Awsat Technical University, Iraq

ARTICLE INFO

Article history:
Received 18 May 2016
Available online 30 November 2016

Keywords:
Adaptive intrusion detection system
Multi-agent system
Real-time
Support vector machine
Extreme learning machine

ABSTRACT

An adaptive intrusion detection system that can detect unknown attacks in real-time network traffic is a major concern. Conventional adaptive intrusion detection systems are computationally expensive in terms of computer resources and time because these systems have to be retrained with known and unknown attacks. In this study, a method called Real-Time Multi-agent System for an Adaptive Intrusion Detection System RTMAS-AIDS, which is based on a multi-agent system, is proposed to allow the intrusion detection system to adapt to unknown attacks in real-time. This method utilizes the classification models multi-level hybrid SVM and ELM to detect normal behavior and known attacks. An adaptive SVM model, in which processes run in parallel and are distributed in MAS, is also used to detect and learn new attacks in real-time. Results show that the proposed method significantly reduced the training cost of detecting unknown attacks compared with the conventional method. In addition, the analysis results of the popular KDDCup'99 dataset show that RTMAS-AIDS can detect Probe, R2L, and U2R attacks better than the non-retrained multi-agent system using the multi-level hybrid SVM and ELM models as well as the multi-level hybrid SVM and ELM. RTMAS-AIDS exhibited a significantly improved detection accuracy that reached 95.86% and can detect and learn unknown attacks faster (up to 61%) than the other two methods (MAS-MLSE and MLSE).

1. Introduction

The security of network and computer systems becomes increasingly important as the amount of sensitive information being stored and deployed online increases. Intrusion detection is an essential component of network and computer security mechanisms. Intrusion detection systems (IDS) aim to identify and respond to malicious activity that compromises network and computer security [1]. Thus, an IDS consists of a detection model that can classify network flow as normal and abnormal. Several researchers have adopted misuse-based detection models that can only detect known attacks, whereas other researchers have presented anomaly-based detection models that can detect known and unknown attacks but with high false-positive rates [2]. The major difficulty encountered in any anomaly-based intrusion detection system is that patterns of normal behavior change over time, and the system must be retrained. An IDS must be able to adapt to these changes in real-time and distinguish normal behavior from intrusive behavior [3].

To reduce false-positive rates and improve the performance of IDS in general, an IDS should be able to detect efficiently and accurately new (unknown) attacks by incorporating knowledge of unknown attacks into a real-time detection model at regular intervals [4]. The ability of conventional IDS to detect new attacks is mostly handled offline manually or semi-automatically [5]. This task requires considerable effort of domain experts in conducting a difficult analysis of audit data and network packets and subsequently inserting these data into the existing deployed models. In the last decades, the interest in data mining and machine learning approaches used to build detection models has increased. These models have been built from normal behavior and known threats to detect unknown threats. They are more automated and faster than manually encoded models. Therefore, information about unknown threats is gathered and promptly incorporated into existing detection models to prevent any further damage from the unknown threats as soon as possible.

Two popular approaches have been proposed to build adaptive IDS [6]. The first one is to generate new forms of unknown threats

[*] Corresponding author at: Data Mining and Optimization Research Group (DMO), Centre for Artificial Intelligence Technology (CAIT), School of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 Bandar Baru Bangi, Malaysia.
E-mail address: wathiqpro@gmail.com (W.L. Al-Yaseen).

http://dx.doi.org/10.1016/j.patrec.2016.11.018
0167-8655/© 2016 Elsevier B.V. All rights reserved.

and then incorporate them with the main detection model. The second is to replace the main detection model with a new detection model built from new and familiar threats. The first approach mainly depends on the features of algorithms in learning unknown threats (e.g., Bayesian network and association rules). The second approach fails because of its slow pace and the fact that it requires a long time to train the detection model every time.

However, network big data is generally associated with the problem of processing large amounts of data, which could arrive in a continuous manner and consider real computing constraints [7]. Hence, the large amounts of network data may require handling in a distributed network, such as the multi-agent system (MAS). MAS is a set of agents that either cooperate or compete to solve a problem. It is utilized to solve complex problems that involve decentralized data, and its tasks are distributed over a number of agents allowed to work autonomously and interact with one another. MAS can reduce system complexity and software costs because the workload is distributed and data analysis is conducted quickly [8]. Given the characteristics of MAS, MAS can be used to design an IDS that cannot be created through a single-agent system. MAS is the most suitable method to achieve the goal in distributed systems [9]. Shamshirband et al. conducted several studies on wireless sensor networks based on MAS. In [8], they assumed that each node is an agent with the ability to make decisions. Each agent collects and processes the information of its environment. When necessary, each agent can provide the collected information to other agents after obtaining permission from the master agent, which is considered an important agent in this method. They also designed a cooperative multi-agent-based fuzzy artificial immune system (Co-FAIS) to protect against DDoS attacks [10]. Co-FAIS is a modular-based defense system that consists of a set of agents working together to calculate the abnormality of sensor behavior or to detect attackers. This system detects misused nodes by using a fuzzy misuse detector module (FMDM) that cooperates with a danger detector module to identify the sources of danger signals. The fuzzy Q-learning vaccination module (FQVM) is utilized to enhance the capability of the system to detect attacks. The cooperative decision-making module (Co-DMM) incorporates the danger detector module with FQVM to produce optimum defense strategies. In addition, they proposed a cooperative multi-agent-based computational intelligence method (MCI-WIDPS) [11]. MCI-WIDPS automatically exchanges data between distributed systems by using software agent techniques. The agents compile data from various sources when an abnormality state has occurred. Thereafter, the managers of the system can make appropriate decisions to prevent this malicious event.

In this study, a multi-agent system for building an adaptive real-time intrusion detection system (RTMAS-AIDS) is proposed. It consists of a detection model and the adaptive model. The detection model uses multi-level hybrid support vector machines (SVMs) and extreme learning machine (ELM) techniques to classify normal and known attack behaviors, whereas the adaptive model employs a single SVM classifier to learn unknown attacks because SVM exhibits good performance in classifying unknown attacks [12]. The goal of using two models is as follows: when an unknown threat is detected, the proposed method does not need to retrain the detection model with unknown and known threats; it only needs to learn the unknown threat and incorporate it into the main detection model. To achieve this objective, we developed the architecture and concepts of a multi-agent system in [13] and used the concepts of the multi-level model, including machine learning classifiers, SVMs, and ELM, in [14].

The remainder of this paper is organized as follows. Section 2 presents related studies on existing adaptive intrusion detection systems. Section 3 describes the proposed system. Section 4 presents the experimental results. Section 5 provides the conclusion and recommendations for future work.

2. Related work

In real-time, the rapid detection of new attacks and the immediate updating of the model are considered the main challenges that researchers face in IDS. This method is known as an adaptive model of IDS, which can be defined as a model that can detect new attacks that have not been identified earlier. Two approaches are used to build an adaptive IDS: generating a new model of new attacks and integrating it into the detection model or replacing the detection model with a newly built one. Many studies related to adaptive IDSs have been conducted.

References [15,4], and [16] used the first approach to build models. Lee et al. [15] conducted a study on real-time data mining-based IDS. They provided several approaches of data mining to address three types of issues. One of them was the usability related to retraining the model on unseen attacks. They proposed generating a lightweight classifier model using the RIPPER method to detect new attacks and then plugging or attaching this model to the existing models. Hossain et al. [4] provided a general framework for an adaptive anomaly detection module. They discussed the major problem of false alarms when modifications exist in the normal behaviors of the system. However, they employed a sliding window method to use the audit data of the sliding window to update the profile. The fuzzy association mining rule was utilized to extract rules of the normal profile. Thereafter, the audit data of the current time window were compared with the profile rule set. When the similarity was above the threshold, the system continued with the current profile without an update. By contrast, the profile was updated with the audit data only in the current time window. A framework that uses the Bayesian network for an adaptive IDS was also proposed by Jemili et al. [16]. In this framework, the association rules of normal connections and known attacks are established from the dataset. These rules generate the learning dataset. Therefore, the connection that is not registered in the learning dataset and has the probability of connection below the threshold is inserted into the learning dataset as a new attack. As a consequence, the learning dataset contains three types of rules: normal, known attacks, and new attacks. Based on this categorization, appropriate security actions are implemented.

Other studies, such as [17,6,18,19,20], and [21], employed the second approach as a basic principle to construct their models. Liao et al. [17] proposed an unsupervised clustering approach to create an adaptive model. They used fuzzy ART and EFuNN techniques as unsupervised clustering learning methods. First, the clusters of normal behavior are established. Second, each input vector is compared with the normal clusters. Consequently, an input vector is assigned to a suitable normal cluster if the similarity is above the threshold and an update of the clusters occurs; otherwise, the vector belongs to the nearest uncertain cluster. After a specified time, if the size of an uncertain cluster reaches the threshold, then that cluster would be added to the normal clusters. Otherwise, the instances of the uncertain cluster will be labeled as an attack, and the uncertain cluster will be deleted. An adaptive tuning model that uses the multi-classifier SLIPPER algorithm was introduced by Yu et al. [6]. This model learns rules with a related prediction confidence ratio for each attack type and normal behavior. The researchers employed the fuzzy controller to update the confidence ratio of the rules. This architecture can reduce false-alarm rates by approximately 20%. Furthermore, Geramiraz et al. [18] presented a detection model based on the fuzzy rules of the normal profile. They employed input variables to present rules by using a genetic algorithm and to provide fuzzy sets by using fuzzy C-means (FCM).