

Active Learning in Cyberspace Security

Pengfei Zhang¹, Zhenyan Liu^{1,*}, Jia Cui², Jingfeng Xue¹, Xinfan Cai¹ and Xiaolei Yang¹

¹ Beijing Key Laboratory of Software Security Engineering Technology,
School of Software, Beijing Institute of Technology, Beijing 100081, China

² China Information Technology Security Evaluation Center, Beijing 100085, China

*Corresponding author

Abstract—At present, machine learning, especially active learning in machine learning, is introduced in cyberspace security field. In this paper, we first analyze the background of cyberspace security and profile active learning. And then we focus on a survey on the application research of active learning in cyberspace security field, mainly including system software security, network security and application security. In the end, we also explore some potential future issues on active learning in cyberspace security.

Keywords—Active learning; Cyberspace security; system software security; network security; application security

I. INTRODUCTION

With the rapid development of information technologies such as the Internet, big data, and cloud computing, the environment faced by cyberspace security is becoming more and more complex, and the security threats it faced are also escalating. Traditional manual methods relied on authoritative experts' experience are difficult to cope with the complicated security problems in current cyberspace. What's more, the introduction of machine learning methods has provided strong support for solving such problems. Currently, combination of machine learning and cyberspace security fields has become a hot spot for experts in academia and industry. More and more latest research progresses which apply machine learning methods to the cyberspace security realm are included in the top four conferences (CSS [1], S&P [2], USENIX [3], NDSS [4]) of the security field. CCS meeting even set up a workshop in order to explore the application of artificial intelligence technology in security and privacy.

Classification is the main task of machine learning, which contains many practical problems, such as the identification of malicious code, the detection of malicious domain names and so on. Classification problem is belonged to typical supervised learning, that is, a large number of data samples with category markers need to be input into the algorithm as the training set. Each sample of the training set contains multidimensional data features and a target variable. The target variable is the predicted result of the machine learning algorithm, and the training sample set must clearly aware the value of the target variable so that the machine learning algorithm can discover the relationship with the data feature. However, in many real-world scenarios, it is difficult to obtain samples with category markers and it need to be manually labeled by experts in related fields, which cost a lot of time and manpower. Moreover, when the training sample is too complex, it will take a long time to process. Therefore, how to quickly and

accurately mark data and get better performance classifiers the major problem needed to be solved urgently has to be solved.

Active Learning has big potential to effectively solve this problem. Active learning is querying the most useful unlabeled samples through a certain algorithm, and marking them by experts, and then training the classification model using the labeled samples to improve the accuracy of algorithm. In this paper, we outline what is active learning in the second section, and then review the research progresses of the application of active learning in the field of cyberspace security from three aspects which are system software security, network security and application security (in the third, fourth and fifth sections). In the final section we summarize this paper and look forward to the future research direction.

II. PROFILING ACTIVE LEARNING

Active learning (sometimes called "query learning" or "optimal experimental design" in the statistics literature) is a subfield of machine learning and, more generally, artificial intelligence [5]. Active learning can independently select unlabeled samples which are the most useful for the learning process to request user tags, and then add these labeled samples to existing training data sets. These new samples can minimize the uncertainty of classifying predictive samples by classifier. Since active learning could reduce the number of redundant samples by selecting a small number of useful unlabeled samples for labeling, so it can greatly accelerate the process.

Generally, active learning could be divided into two parts: learning engine and selection engine. The learning engine maintains a benchmark classifier and can improve the performance of the classifier through learning the labeled samples provided by supervised learning algorithms, while the selection engine is responsible for running the sample selection algorithm to select an unlabeled sample and hand it over to human experts to mark and then adds the marked sample to the marked sample set. After repeated cycles of alternately working of the learning engine and the selection engine, the performance of the benchmark classifier is gradually improved. Finally, the process terminates when the preset conditions are met.

Active learning can be modeled by the following five components:

$$A = (C, L, S, Q, U)$$

Where C is a classifier or a group of classifiers; L is a data sample set with category tags; S is a supervisor, which can mark unlabeled samples; Q is a query function for querying the sample which has the largest amount of information (most useful) in unlabeled samples; U is the entire unlabeled sample set.

The active learning process consists of two phases (as shown in Figure 1): the first phase is the initialization phase, a small number of random unlabeled samples are selected, and the supervisors mark them as the training set to establish the initial classification model; the second phase is the loop query phase, a certain unlabeled sample which is in the unmarked sample set U is selected for labeling by S according to a certain query criterion Q , then added to the training sample set L , and the classifier is retrained until the training stop criterion is reached.

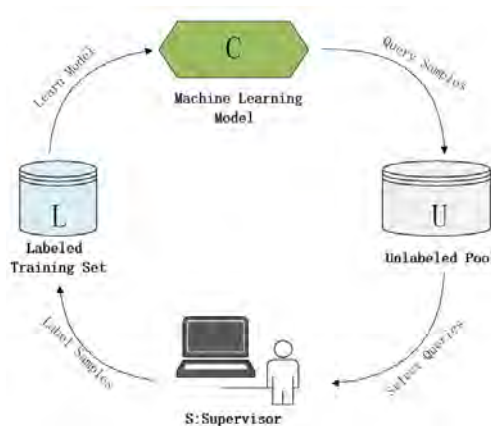


FIGURE 1. THE PROCESS OF ACTIVE LEARNING

Active learning can be divided into two types based on the way of untapped samples obtained: stream-based and pool-based. In stream-based active learning, the selection engine decides whether to mark the current submitted samples where unlabeled samples are submitted to the selection engine one by one in order. In pool-based active learning, a collection of unlabeled samples is maintained, and the selection engine selects which sample need to be marked from the collection.

The core selection strategies mainly include the following strategies:

1) *Uncertainty Sampling*: Uncertain sampling is probably the simplest and most common active learning query strategy. The sample with the largest amount of information is selected from the sample pool and submitted to the expert to label its category information. This method reduces the classification uncertainty of the classifier to a certain degree and can greatly improve the accuracy of the classifier. Lewis [6] uses a classifier to select samples with a class posterior probability close to 0.5 to join the training set, and each time the most uncertain sample of the classifier is selected to join the training set, with the classifier's classification error increased.

2) *Query-By-Committee*: Seung [7] proposed the committee voting selection algorithm. This method does not directly calculate the classification error. Instead, it first

establishes two or more classifiers based on the existing class label data to form a "committee" and uses this committee to label the prediction samples. Then it selects the most inconsistent sample as the candidate sample. This method can add samples with rich information to the training set, the computational complexity is relatively low, the learning speed is fast, and a small number of training samples can achieve the desired accuracy. The QBC selection strategy is based on how to reduce the search space (Version Space). It is relatively simple to calculate (only one inner product is needed when evaluating each unlabeled sample), and the algorithm tends to select sample data which can be divided search space into two approximate size parts. When such samples are added to the training set, one part is removed from the entire search space, which speeds up the learning process.

3) *Expected Error Reduction*: Roy and McCallum [8] first proposed error reduction method in the text classification using the naive Bayesian method. Zhu et al. [9] combined this framework with a semi-supervised learning approach, resulting in a dramatic improvement over random or uncertainty sampling. Guo and Greiner [10] employed an "optimistic" variant that biases the expectation toward the most likely label for computational convenience, using uncertainty sampling as a fallback strategy when the oracle provides an unexpected labeling.

4) *Variance Reduction*: Variance Reduction, as its name suggests, intends to minimize the model error rate by selecting instances with the minimum variance [11]. This type of methods often takes advantage of a statistical model measuring Fisher Information to evaluate the variance, which is a partial derivative of the log-likelihood function with regard to a model parameter. Minimizing the variance over its parameter estimation is equivalent to maximizing the Fisher Information Function. The advantage of this kind of approach is that the information matrices representing the variance simulate a model retraining process. There are also some practical disadvantages, such as computational complexity.

In recent years, more and more researchers have committed to applying active learning to the field of cyberspace security. In particular, there are a lot of research progresses in the sub-areas of cyberspace security including system software security, network security and application security. Next, we will discuss the typical research results of active learning in the field of cyberspace security and focus on these three sub-areas.

III. ACTIVE LEARNING IN SYSTEM SOFTWARE SECURITY

Systems in cyberspace mainly refer to unit computing systems with independent computing capabilities, such as computers, mobile terminals, and the like. This section mainly introduces the research results of active learning in system software security, including vulnerability analysis and mining and malicious code analysis.

A. Vulnerability Analysis and Mining

Vulnerability refers to the defects and deficiencies which exist in the specific implementation of system in hardware, software and protocols or in the design of system security policies, thus threatening and damaging the security of the unit

computing system. From the earliest Morris worm to the WannaCry ransomware that broke out in May 2017, the system was attacked through exploiting system vulnerabilities and network is the way of transmission. Therefore, vulnerability identification in system software is undoubtedly the key point in the research of cyberspace security. Vulnerability identification research has been conducted for many years, such as identifying through the characteristics of the vulnerability, random testing techniques (such as fuzzing), and analysis methods such as static analysis and symbolic execution.

At present, in terms of vulnerability discovery and prediction, researchers have achieved some results in combination with active learning methods. V. D. L. Wesley and V. Siccio [12] proposed a learning state machine testing technique using active learning to detect vulnerabilities in Android applications. Active state machine learning consists of learners and teachers. The goal of the learner is to infer the state machine model of the system under test by asking the teacher for membership queries and equivalent queries. The combination of active learning and learning algorithms can reduce unnecessary queries, reduce query space, and optimize the time required to interact with equivalent models.

Z. Yu et al. [13] present an incremental vulnerability prediction tool called HARMLESS, which is the first tool using active learning in the arena of vulnerability prediction. HARMLESS assumes no training data is available when the security review and test starts. It applies active learning to prioritize the security review and test effort on the source code files most likely to contain vulnerabilities, reflecting on the security review and test results seen so far. As a result, it can achieve recalls over 90 to 99% in the cost of reviewing 24% to 45% of the source code files.

B. Malicious Code Analysis

Malicious code usually refers to applications with malicious features, including Trojans, worms, viruses, and so on. Malicious code analysis usually divided into static analysis and dynamic analysis. Static analysis analyzes the program's instructions and structure to determine whether it has malicious functions, while dynamic analysis analyzes the running behavior in an isolated environment (such as simulator, sandbox) to determine whether it has malicious functions. At present, many studies have used active learning techniques to analyze malware with a large amount of code, complex code features, or complex operational behavior.

Mao et al. [14] proposed a malicious code detection method that uses active learning with minimizing estimated risk. This method is based on the strategy of estimating risk minimum, incrementally actively learning unknown samples, and constantly improving the malicious code detection classifier. A small number of known samples are needed to get better malicious code detection. The experimental results show that compared with the traditional statistical classifier-based method, the active learning method improves the malicious code detection effect. In the case of only 1% sample, the detection error rate is reduced by 36.5%.

Robert et al. [15] presented a complete methodology for the detection of unknown malicious code which using an Active-

Learning framework that enables the selection of the unknown files for fast acquisition. They implemented two selective sampling (pool-based) AL methods: the Simple Margin presented by Tong and Koller and Error Reduction presented by Roy and McCallum. The first method is directly oriented to the SVM classifier, and the Error Reduction method is more general and can be applied to any classifier that can provide probabilistic values for its classification decision. Then they defined specific evaluation measures based on the known precision and recall measures, which show the accuracy of the acquisition process and the improvement in the classifier resulting from the efficient acquisition process.

N. Nissim et al. [16] proposed a technique based on computer measurements extracted from the operating system. They applied support vector machines to the resulting feature subsets. In addition, they used active learning as a selective sampling method to increase the performance of the classifier and improve its robustness in the presence of misleading instances in the data. The results indicate a mean detection accuracy in excess of 90%, and an accuracy above 94% for specific unknown worms using just 20 features, while maintaining a low false-positive rate when the active learning approach is applied.

Gradually, with the development of mobile applications, malware detection on the mobile side has become a research hotspot. H. Zhu [17] proposed an active learning framework to solve the problem that a lot of Android examples cost much to mark manually. In the active learning framework, Naïve Bayes, Decision Tree, Logistic Regression and Support Vector Machines are used to mark the labels for Android examples. The experiments indicated that the active learning framework can effectively detect Android malware.

B. Rashidi et al. [18] presented an Android malicious application detection framework based on the Support Vector Machine (SVM) and Active Learning, in which they use Expected error reduction query strategy to integrate new informative instances of Android malware and retrain the model to be able to do adaptive online learning. And the results showed that the approach can accurately detect malicious applications and improve updatability against new malware.

N. Nissim et al. [19] introduced an active learning framework, "ALDROID", to detect new unknown Android malware. And they present a set of general descriptive features which are robust and unaffected by obfuscation or transformation evasion techniques. The features are based on the application's static genes and not on the optional operations it might conduct. Their AL methods acquired the largest number and percentage of new malwares, while preserving the detection models' detection capabilities (high TPR and low FPR rates).

IV. ACTIVE LEARNING IN NETWORK SECURITY

The various detection measures in network security which is an important pillar of cyberspace security provide secure communication guarantee for the development of numerous activities of the Internet. This section mainly introduces the research results of active learning in network security detection, including the application of active learning technology in BGP

(Border Gateway Protocol) anomaly detection, botnet detection and network intrusion detection.

A. Anomaly BGP Detection

The Border Gateway Protocol is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet and is involved in making the core routing decisions of the Internet. The problem is, it cannot verify the integrity and authenticity of the routing information declared by the Autonomous System because of lacking a secure and reliable route authentication mechanism. This defect causes routers to face multiple attacks, such as Prefix Hijacking and abnormal BGP update messages, which seriously affect the connectivity and security of the Internet.

The abnormal route is detected by extracting the current BGP update message's feature or timing feature, then identified as a normal route or an abnormal route. Wu and Feng[20] proposed a method that contain active learning based on the under-sampling and asymmetric bagging to classify BGP routing dynamics and detect abnormal data. Under-sampling is used in training neural networks and asymmetric bagging is used to improve the accuracy of the algorithm. The experiment shows that this method is a powerful technique to this field compared with other 4 methods.

B. Botnet Detection

A botnet is a logical collection of internet-connected devices such as computers, smartphones or IoT devices whose security has been breached and control ceded to a third party. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection. The activities of botnets are mainly divided into three stages: communication, command and control (C&C) which is the core working mechanisms of botnets, and attack. Traditional botnet detection uses manual analysis method which is a very inefficient technique because different botnets have different propagation, command and control, and attack methods.

Qiu et al. [21] applied an active learning (AL) framework for botnet detection, facilitating detection of unknown botnets. Unlike previous studies, their approach judiciously involves a human-in-the-loop (network security administrator) to help label certain of a current batch of bidirectional flows, i.e. Experiments on real world network traffic data, including several common botnet instances, demonstrate the advantage of their proposed features and AL system.

Some studies are based on the membership query method in active learning. Cho et al. [22] presented an application of active automata learning in the security space that received a lot of attention: using L^* , they inferred a formal model of the command and control protocol of a botnet. They designed an effective protocol inference system and provided empirical evidence that their optimizations — query response prediction, parallelization, and caching—speed up the inference process by over an order of magnitude compared to the basic L^* algorithm. Compared with other methods, this method reduces the number of queries and reduces the learning time.

C. Intrusion Detection

Intrusion detection judges the normal behavior or abnormal behavior of the system according to the network traffic data or the number of hosts. It can be abstracted into classification problems, where a classifier is constructed by learning the training set to distinguish normal behavior from abnormal behavior. As the core technology of intrusion detection system, intrusion detection directly affects the efficiency, false alarm rate and detection effect of the attack. Intrusion detection is mainly divided into two categories: anomaly detection technology and misuse detection technology. Anomaly detection technique constructs a model representing normal behavior from a given normal training data set, and all events that do not conform to this model are suspected of being an attack. It is sensitive to new types of attacks, can effectively detect new attacks, and can detect zero-day vulnerabilities. However, the learning of the normal behavior pattern of the system is usually complicated, thus the established abnormal detection system may generate a high false alarm rate for unknown attacks. Misuse detection distinguishes intrusion behavior from normal behavior by known characteristics which are acquired from known attacks. Compared to anomaly detection, it has high efficiency but low false positive rate, can only discover the known intrusion, and the maintenance of features is mostly done manually.

Liu et al. [23] proposed an anomaly detection method based on single-class support vector machine and active learning. Firstly, the single-class support vector machine model is established in an unsupervised manner, and then abnormal samples are selected by the active learning strategy to be labeled, and the model data is extended and optimized in a semi-supervised manner to determine the new classification boundary. Secondly, the selection strategy and termination conditions of the active learning are studied: the confidence of the sample need to be considered while the sample is selected and considering the role of labeled and unlabeled samples while setting termination conditions. The combine with active learning method optimized the performance of the model with a small marking cost and obtained a large performance improvement at a small cost.

Yang Li and Li Guo[24] propose a novel supervised network intrusion detection method based on TCM-KNN (Transductive Confidence Machines for K-Nearest Neighbors) machine learning algorithm and active learning based training data selection method. In their algorithm, the two most widely used active learning methods are described, namely uncertainty-based sampling and query by committee. And they make contrast experiments between TCM-KNN algorithm and the classical algorithms commonly effectively used in intrusion detection, including SVM algorithm, neural networks, and KNN (K-Nearest Neighbors) algorithm. The experiments showed that the performance of their method is good both on original KDD 99 (TP=99.7%, FP=0) and on the data set after employing feature selection (TP=99.6%, FP=0.1%).

In [25], Seliya and Khoshgoftaar proposed a neural network based active learning method. Regularization-based network was utilized and a performance function was built based on the network errors to improve generalization of the feedforward neural network. The experiments on DARPA KDD-1999

intrusion detection project demonstrate that it can obviously reduce the size of training data, without dramatically decreasing the classification accuracy. Furthermore, the classification performance from neural network-based active learning is comparable to that of supervised C4.5 decision tree.

Long et al. [26] proposed a novel active cost-sensitive learning method for intrusion detection using the technologies of active learning and cost-sensitive learning. The proposed method uses a popular cost-sensitive learning method Meta cost as the base classifier and a sampling criterion of the largest misclassification cost. The results of the experiments on intrusion detection datasets of KDDCUP 99 show that the proposed method is effective.

K. Valli and Ravi [27] demonstrated a hybrid semi-supervised machine learning technique that uses Active learning Support Vector Machine (ASVM) and Fuzzy C-Means (FCM) clustering in the design of an efficient IDS. There are primarily two phases in the proposed approach, if the SVM classifier has decided the input sample under test to be abnormal, then FCM is used to find the sub categories based on the previously generated FCM clusters in the training phase. The nearest circle with higher fuzzy membership is chosen as its sub class. NSL-KDD data set is used for testing the proposed algorithm and an accuracy of 99.6% is recorded.

Steven [28] proposed an Active Learning Intrusion Detection System (ALIDS) machine learning algorithm that applies active learning to the task of intrusion detection. ALIDS consists of a random forest classifier, which is trained using the active learning trainer. The trainer is also responsible for evaluating the classification results, determining the sample that will be sent to the oracle, and retraining the classifier using previously discovered labels as well as new labels provided by the oracle. Rather than a human reviewing and labeling 4.9 million records, ALIDS requires a human to label only 6,465 (0.13%) of those records and automatically classifies 90% of the records.

V. ACTIVE LEARNING IN APPLICATION SECURITY

The security of software applications such as email, PDF, web pages, etc. are one of the hot issues that researchers concerned about. This section describes the active learning related research in software application security, including spam detection, URL-based malicious web page recognition, and Malicious PDF detection.

A. Spam Detection

The traditional spam detection method manually set the detection rule on the server side, which complete the spam filtering through modifying the mail transmission protocol on the server side to set the sending or receiving rules or set the black and white list. This method can only block known types of spam, so the detection efficiency is low and the rules can't be updated in time. The problem of traditional spam detection methods can be solved by using active learning technology that could automatically update rules.

Many pool-based active learning methods have been applied to spam filtering and have acquired a very good effect.

KL Li et al. [29] for the first time proposed a method for spam categorization based on support vector machines (SVMs) using active learning strategy. In their paper, instead of using a randomly selected training set, the learner has access to a pool of unlabeled instances and can request the labels for some number of them.

W. Liu and T. Wang [30] proposed a SVMEL (SVM Ensemble Learning) method to combine five simple filters for higher accuracy and use active learning method to choose training emails for less training time. Using uncertainty-based sampling (UBS) method they choose those emails whose ensemble SCS (spam confidence score) is about 0.5. The experiments results show the filter applying active learning method can reduce requirements of labeled training emails and reach steady state performance more quickly.

N. Chen and Z. M. Tang [31] proposed spam filtering a method which is based on query-by-committee algorithm and can dynamically increase the sampling threshold. In order to reduce the number of sampling, the high-information training sample which belongs to unlabeled sample pool is obtained step by step, the voting entropy is used to measure the uncertainty of the sample category attribution, and the sample whose entropy exceeds the threshold θ is labeled and learned. With the enhancement of classifier predictive ability, threshold was increased by $\Delta\theta$. As a result, the labeling cost and learning time cost which is brought by sample collection was reduced, and there's no significant impact on classification accuracy.

J. M. Xu et al. [32] proposed a method which is based on clustering unlabeled emails, querying the label of one email per cluster, and propagating such label to the most similar emails of the same cluster. The effectiveness of the method is evaluated using the well-known open source "SpamAssassin" filter, on a large and publicly available corpus of real legitimate and spam emails.

Some scholars have applied online active learning to spam detection. D. Sculley [33] investigated an online active learning scenario where the filter is exposed to a stream of messages which must be classified one at a time. In the paper, they describe several online active learning active strategies for linear classifiers and test these methods on spam filtering tasks using three linear classifiers: classical Perceptron, Perceptron with Margins, and linear Online Support Vector Machines. The result shows that these methods greatly reduced the number of labels needed to achieve strong classification performance on two large benchmark data sets.

In [34], W. Liu and T. Wang proposed an online active multi-field learning approach, which try to integrate online learning, multi-field learning, and active learning to form an improved approach. In the active learning part, they use uncertainty sampling, which selects those easily incorrectly classified samples for training. And they use the multi-field text structure to break a complex problem into multiple simple sub-problems. The experimental results show that the proposed approach can achieve the state-of-the-art performance with greatly reduced label requirements and very low space-time costs.

B. URL-based Malicious Web Page Recognition

Malicious Web page usually refers to a collection of web pages that can steal user privacy, install malicious programs, or execute malicious code when a user visits it. Malicious Web page recognition usually adopts a blacklist-based identification method, a rule-based matching method or a host-based behavior recognition method. These methods still exist some problems such as poor timeliness, high false positive rate, and difficulty in updating. With its powerful self-learning ability, combination of active learning and classification algorithms has become a new technical route in the research of malicious web page recognition.

He et al. [35] proposed an active learning algorithm based on URL-based Support Vector Machine (SVM), which is used to implement phishing detection. Firstly, filtering the URL to the blacklist or whitelist and classifying the suspicious URLs that are neither in the blacklist nor in the whitelist. In order to adapt to the classification model of the small sample set and ensure the detection efficiency of the classifier, the active learning algorithm with the support vector machine is adopted to reduce the number of training samples of the classifier and to improve classification performance and efficiency by learning and screening the training samples.

P. Zhao et al. [36] presented a novel framework of Cost-Sensitive Online Active Learning (CSOAL), which only queries a small fraction of training data for labeling and directly optimizes two cost-sensitive measures to address the class-imbalance issue. Through conducting an extensive set of experiments to examine the empirical performance of the proposed algorithms for a large-scale challenging malicious URL detection task, in which the encouraging results showed that the proposed technique by querying an extremely small-sized labeled data (about 0.5% out of 1-million instances) can achieve better or highly comparable classification performance.

Sreyasee et al. [37] proposed an effective active learning approach that can efficiently address this limitation in a practical cyber-security problem of Phishing categorization, whereby they use a human-machine collaborative approach to design a semi-supervised solution. Prioritized Active Learning shows a significant promise to achieve faster convergence in terms of the classification performance in a batch learning framework, and thus requiring even lesser effort for human annotation. In experiments with several collections of dataset, the proposed method shows significant improvement over the baseline by as much as 12%.

C. Malicious PDF Detection

Malicious PDF refers to a normal PDF file embedding malicious code. Traditional malicious PDF detection methods which are low recognition rate and inability to update malicious code in time are based on virus detection, signature-based detection methods, etc. Active learning technology provides a new direction for malicious PDF detection. Similar to malicious web page recognition, the detection of malicious PDF software is also a two-class problem of machine learning, but the features adopted by the two are significantly different.

N. Nissim et al. [38] presented ALPD, a framework based on active learning methods that focuses on improving anti-virus

by labeling those PDF files and it is labeled by a human expert. In their framework, two active learning methods, "Exploitation" and "Combination" were introduced. "Exploitation," is based on SVM classifier principles and is oriented towards selecting examples most likely to be malicious that lie furthest from the separating hyperplane. The "Combination" method lies between SVM-Margin and Exploitation. The results showed that using Combination and Exploitation, 93.5% and 92.5% of the acquired files were malicious.

VI. CONCLUSIONS AND FUTURE DIRECTIONS

Security threats and protection issues of cyberspace is not only related to national security, but also closely related to people's daily lives. Active learning, as one of the most hot research goal in the field of machine learning, has achieved a series of remarkable research results of image recognition and speech recognition and attracted more and more attention. In this paper we systematically summarize and analyze these results. Cyberspace security research based on active learning has achieved many solutions and methods in system security, network security and application security, and good detection effects have been obtained in the field of malicious code detection, network intrusion detection and spam detection, etc.

However, there are still a few problems difficult to solve and needed further research. It is still extremely challenge to use active learning technology to solve the cyberspace security problems. The active learning technology has certain research difficulties: when the dimension of the input data is very high, it will face the problem of "dimensionality disaster" in high-dimensional space. So, it is necessary to find an efficient dimensionality reduction algorithm in the preprocessing stage to reduce query complexity [39]. Further research on the application of active learning include: 1) combining a priori knowledge of specific application areas and studying more efficient active learning algorithms to reduce the cost of labeling samples. 2) Combining other technologies such as cost-sensitive learning and Unbalanced data sets Learning to effectively deal with problems in the field of cyberspace security [40].

ACKNOWLEDGMENT

This work was financially supported by Scientific Research Project of Beijing Institute of Technology (2017CX02029).

REFERENCES

- [1] <http://www.sigsac.org/ccs.html>
- [2] <http://www.ieee-security.org/TC/SP-Index.html>
- [3] <https://www.usenix.org>
- [4] <https://www.ndss-symposium.org>
- [5] B. Settles, "Active Learning Literature Survey," University of Wisconsin-Madison, 2009, pp. 127–131.
- [6] D. Lewis and W. Gale, "A sequential algorithm for training text classifiers," In Proceedings of the ACM SIGIR Conference on Research and Development in Information Retrieval, ACM/Springer, 1994, pp. 3–12.
- [7] B. Settles, M. Craven and L. Friedland, "Active learning with real annotation costs," In Proceedings of the NIPS Workshop on Cost-Sensitive Learning, 2008, pp. 1–10.

- [8] N. Roy and A. McCallum, "Toward optimal active learning through sampling estimation of error reduction," In Proceedings of the International Conference on Machine Learning (ICML), Morgan Kaufmann, 2001, pp. 441-448.
- [9] X. Zhu, J. Lafferty, Z. Ghahramani, "Combining active learning and semi-supervised learning using Gaussian fields and harmonic functions," In Proceedings of the ICML Workshop on the Continuum from Labeled to Unlabeled Data, 2003, pp. 58-65.
- [10] Y. Guo and R. Greiner, "Optimistic active learning using mutual information," In Proceedings of International Joint Conference on Artificial Intelligence (IJCAI), AAAI Press, 2007, pp. 823-829.
- [11] Y. Fu, X. Zhu and B. Li, "A survey on instance selection for active learning," Knowl. Inf. Syst. vol. 2, 2013, pp. 249-283.
- [12] V. Wesley, V. Sicco, "Vulnerability Detection in Mobile Applications Using State Machine Modeling," IEEE European Symposium on Security and Privacy Workshops, 2018, pp. 1-10.
- [13] Z. Yu, C. Theisen, H. Sohn, L. Williams, T. Menzies, "Cost-aware Vulnerability Prediction: the HARMLESS Approach," In Proceedings of The 26th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2018). ACM, New York, NY, USA, 2018, pp. 1-11.
- [14] W. X. Mao, Z. M. Cai, L. Tong, "Malware detection method based on active learning," Ruan Jian Xue Bao/Journal of Software, 2017, pp.384-397 (in Chinese), <http://www.jos.org.cn/1000-9825/5061.html>.
- [15] R. Moskovitch, N. Nissim, Y. Elovici, "Acquisition of malicious code using active learning," In Proc. 2nd Int'l Workshop on Privacy, Security, & Trust in KDD, Las Vegas, NV, USA, 2008.
- [16] N. Nissim, R. Moskovitch, L. Rokach, Y. Elovici, "Detecting unknown computer worm activity via support vector machines and active learning," Pattern Analysis and Application, vol. 4, 2012, pp. 459-475.
- [17] H. Zhu, "Active learning framework for android unknown malware detection," International Conference on Automotive Engineering, 2017, pp. 345-348.
- [18] B. Rashidi, C. Fung and E. Bertino, "Android malicious application detection using support vector machine and active learning," International Conference on Network & Service Management, 2018, pp.1-9.
- [19] N. Nissim, R. Moskovitch, O. BarAd, L. Rokach and Y. Elovici, "Aldroid: efficient update of android anti-virus software using designated active learning methods," Knowledge and Information Systems, vol. 3, 2016, pp. 795-833.
- [20] Q. Wu and Q. Feng, "Abnormal BGP Routing Dynamics Detection by Active Learning Using Bagging on Neural Networks," Springer Berlin Heidelberg, vol. 6, 2009, pp. 931-936.
- [21] Z. C. Qiu, D. J. Miller and G. Kesidis, "Flow based Botnet Detection through Semi-Supervised Active Learning," Tech. Rep.CSE-16-010, CSE Dept., PSU, Sept. 12, 2016,<http://www.cse.psu.edu/research/publications/techreports12016/CS-E-16-010.pdf/pdf/view>.
- [22] C. Y. Cho, D. Babić, E. C. R. Shin, and D. Song, "Inference and analysis of formal models of botnet command and control protocols," In Proceedings of the Conference on Computer and Communications Security, 2010pp. 426-439.
- [23] J. Liu, L. Gu, X. Niu, Y. X. Yang, "Research on network anomaly detection based on one-class SVM and active learning," Information Security Center, vol. 11, 2015, pp. 136-146.
- [24] L. Yang, G. Li, "An active learning based TCM-KNN algorithm for supervised network intrusion detection", Elsevier Advanced Technology Publications, vol. 7, 2007, pp. 459-467.
- [25] N. Seliya and T. M. Khoshgoftaar, "Active learning with neural networks for intrusion detection," in Information Reuse and Integration (IRI), 2010 IEEE International Conference on. IEEE, 2010, pp. 49-54.
- [26] J. Long, J. P. Yin, E. Zhu, W. T. Zhao, "A novel active cost-sensitive learning method for intrusion detection," in: 2008 International Conference on Machine Learning and Cybernetics, 2008, pp. 1099-1104.
- [27] V. V. Kumari, P. R. Varma, "A semi-supervised intrusion detection system using active learning SVM and fuzzy c-means clustering," In ISMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE, International Conference on 2017 Feb 10, 2017, pp. 481-485.
- [28] M. Steven, "Active learning intrusion detection using k-means clustering selection", SoutheastCon 2017, Charlotte, NC, USA, 2017.
- [29] K. L. Li, K. Li, H. K. Huang, S. F. Tian, "Active learning with simplified SVMs for spam categorization," International Conference on Machine Learning & Cybernetics, vol. 3, 2002, pp. 1198-1202.
- [30] W. Y. Liu, T. Wang, "Active Learning for Online Spam Filtering," Springer Berlin Heidelberg, 2008, pp. 555-560.
- [31] N. Chen, Z. M. Tang, "Method of spam filtering online based on QBC active sampling learning algorithm," Computer Engineering and Applications, vol. 22, 2014, pp. 170-174.
- [32] J. M. Xu, G. Fumera, F. Roli, Z. H. Zhou, "Training SpamAssassin with Active Semi-supervised Learning," CEAS 2009 - Sixth Conference on Email and Anti-Spam July 16-17, 2009, Mountain View, California USA.
- [33] D. Sculley, "Online Active Learning Methods for Fast Label-Efficient Spam Filtering," Ceas -the Fourth Conference on Email & Anti-spam, 2007.
- [34] W. Liu, T. Wang, "Online active multi-field learning for efficient email spam filtering," Knowledge & Information Systems, vol. 1, 2012, pp. 117-136.
- [35] G. He, F. Zou, D. Tan, M. Wang, "Phishing Detection System Based on SVM Active Learning Algorithm," Computer Engineering, vol. 19, 2011, pp. 126-128.
- [36] P. Zhao and S. C. Hoi, "Cost-sensitive online active learning with application to malicious url detection," in Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2013, pp. 919-927.
- [37] S. D. Bhattacharjee, A. Talukder, E. A. Shaer, P. Doshi, "Prioritized Active Learning for Malicious URL Detection using Weighted Text-Based Features," IEEE International Conference on Intelligence & Security Informatics, 2017.
- [38] N. Nissim, A. Cohen, M. Robert, A. Shabtai, M. Edry, B. Oren, Y. Elovici, "ALPD: Active Learning Framework for Enhancing the Detection of Malicious PDF Files," Intelligence & Security Informatics Conference, 2014, pp. 91-98.
- [39] K. Liu, X. Qian, Z. Q. Wang, "Survey on active learning algorithms," Computer Engineering and Applications, vol. 34, 2012, pp. 1-4.
- [40] J. Long, J. P. Yin, E. Zhu, W. T. Zhao, "A Survey of Active Learning," Journal of Computer Research and Development, vol. 45, 2008, pp. 300-304.