Security Evaluation Research of Mobile Payment Application Based on SVM

Yang Liu, Juan Xu, Hui Fei, Yanhui Guo, Guoai Xu
(Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876)

Abstract: With the increase of mobile payment malicious applications, an accurate assessment of their safety is particularly important. In recent years, machine learning methods have achieved good results in text recognition, medical diagnosis, anomaly detection and other fields. Therefore, we consider the introduction of the application of many features including application signature information, application permissions, suspicious API, special string to construct a sample feature space and evaluate the safety of mobile payment applications based on support vector machine algorithm. By comparing the accuracy of a variety of algorithms, the algorithm is turned to be feasible. The importance of the evaluation index is different during the sample classification and there is a difference in the performance of the kernel function under different conditions. So this paper studies the performance of the classifier in different evaluation index set, kernel function and feature weights. It proves that the polynomial kernel support vector machine method is best based on feature weights after the introduction of four types of evaluation index. This method properly avoids the problem of low accuracy due to a single feature while eliminating the adverse effects of weak correlation evaluation index.

Key words: Support vector machine; Kernel function; Feature weights

I. INTRODUCTION

With the development of mobile Internet, mobile payment is becoming increasingly popular. Domestic banks and third-party payment companies have released applications for mobile payment. At the same time, a large number of mobile banking, third-party payment application is implanted virus by secondary packaging. This seriously do harm to the user property. Compared with games, social applications, the third-party payment applications are more dangerous, thus it is necessary to assess its safety effectively. Previous study of mobile payment mostly concentrated in the direction of data security, such as mobile payment authentication method, security protocol and data encryption, etc. These directions ignore the security of the application itself. Therefore, using the method of data mining, this paper evaluates the safety of the application through analyzing the characteristic of application.

SVM (Support Vector Machine) is a data mining method proposed by Corinna Cortes and Vapnik in 1995, which has been successfully applied in many fields. In order to solve the problem of safety evaluation on mobile payment application, this paper proposed a multiple characteristics of support vector machine (SVM) model based on mobile payment application. To build high-performance, high-reliability evaluation model, this paper mainly formed from the following aspects: First, study mobile payment application features, determine the evaluation index of samples, including signature information, application permissions, suspicious API, special string. Second, under the same conditions, test the accuracy and stability of various algorithms, prove that support vector machine is more suitable than other methods. Third, studythe influence of different evaluation collections, different kernel functions, different features weights on SVM classification, then confirm the best feature set of samples by a combination of different evaluation

© 2016. The authors - Published by Atlantis Press

experiments. Change the kernel function of classification model, compare their accuracy, thus to select the most suitable kernel function for this paper. Alter the character weights, highlighting the role of strong correlation characteristics, eliminate the influence of weak correlation characteristics to optimize classification performance.

II. RELATED PROBLEM

A. *Related Research*

Currently, the artificial judge of mobile payment application security mainly start with analysis from the signature information, application permissions, API calls and other features. But in fact, many of these features, are hard for manual analysis and easy to lead to false positives. Data mining techniques can excavated meaningful information from large amounts of data. Mobile application security assessment is a typical two-class problem. It can be abstracted into machine learning model, where the application security assessment can be abstracted as follows: Known application features set {S1, S2, S3 …}, application security set {malice, normal}, specifically as shown in Figure 1. For the machine learning model, select an appropriate classification algorithm is very important.

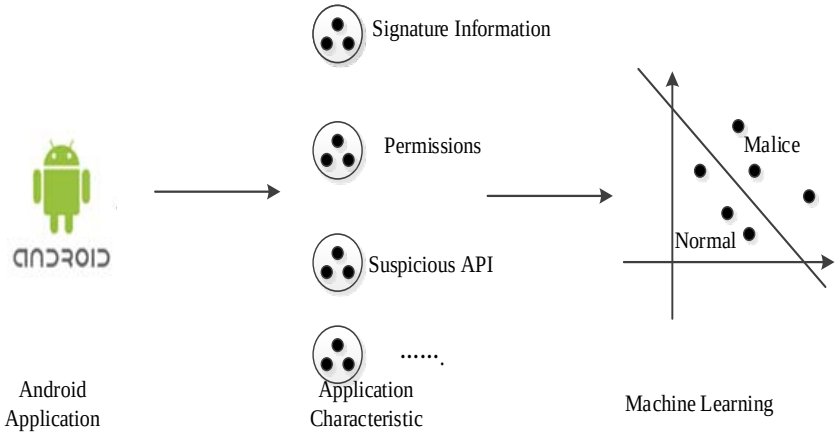

Fig. 1 Mobile payment application assessment model

Study the application of recent data mining algorithms on mobile application, we found that document [4] proposes permission-based feature Naive Bayes and its improved algorithms to assess the applications. This method is simple, but its evaluation is single and can cause high miscalculation. In addition, Bayesian algorithm relies on sample distribution, and the correlation and redundancy of attributes will greatly reduce the classification accuracy. Document [5] uses application permissions, application group price, suspicious API as a sample feature space, and then introduces K-means clustering algorithm and K nearest neighbor classification algorithm to process mobile application classification problems. Compared to document [4], document [5] increases the application components and suspicious API, and has a higher accuracy rate. But K-nearest neighbor method is a learning method based on instance. When processing test samples, K-nearest neighbor method needs to individually calculate the similarity between test samples and training samples. This will lead to greater processing overload, and the classification performance will be easily interfaced by the noise data. Taking the following advantages of SVM into account, this paper chooses support vector machine as the classification method. On one hand, it can take advantage of the nonlinear transformation to map the large number of applications to a high dimensional feature space, and effectively reducing the input space dimension and complexity of algorithm, to avoid over-learning, local minima and curse of dimensionality. On the other hand, according to their structural risk minimization principle, converse the classification problem into quadratic optimization problems to find the optimal hyperplane under certain constraints. This can avoid classification model depends on the prior probability of the sample, and effectively improve the accuracy and stability of

classification model in case of small sample. In order to establish a good assessment model, the next step will study the mobile payment application features, and choose index to build sample feature space.

B. Evaluation

In order to select a fine evaluation, this paper incorporated by reference [4] [5], will use application permissions and suspicious API as evaluation index. The purpose of application component in document [5] is to associate with suspicious API. It will bring feature redundant questions, and you can determine whether suspicious API directly associated with the application components when extract features. Thus, it can improve the classification efficiency. In addition, the application also has following characteristics: First, the signature information can prove whether the application has been tampered with. Second, mobile payment applications general presence backstage send text message, e-mail and uninstall security software and other acts, resulting in possible special string like phone number, email in malicious applications. The paper has added two more evaluations indicators: signature information, special string.

1 Signature Information

Each mobile application contains a piece of signature information, which represents the issuer of the application. Thus, by comparing the APK's signature, you can determine whether the APK from the "official" issue, rather than re-signing cracked tampered packaged "pirated software". Further, due to the presence of leaked signature information, this paper adds the following evaluation index.

2 Application Permissions

Android permission system is setted up to ensure the authorized use of system resources. For example, to send text message, normal or malicious applications all need to apply for SEND_SMS permission. Currently, there are a total of 114 kinds of Android application permissions, and different types of applications use different permissions. According to the analysis results of document [6], you can obviously find the financial application requests about 22 permissions. But in these 22 kinds of privileges, there are permissions which can not cause malicious acts. Therefore, this paper analyzes the use of malicious mobile payment application permissions and the necessary permissions of common malicious programs, and selects the following 13 kinds of privileges as the evaluation index:

Tab. 1Permissions feature

Privilege Categories	*Privilege Function*
RECEIVE_SMS	Allow SMS monitoring and SMS forwarding function
READ_CONTACTS	Allow reading contacts
SEND_SMS	Allow sending text message
READ_PHONE_STATE	Allow listening mobile phone calls, to achieve monitor conversations
INJECT_EVENTS	Allow users to intercept events such as keys, touch, trackball, etc.
INTERNET	Allow network connections, GPRS traffic may be generated
WRITE_EXTERNAL_STORAGE	Allow the program to write to the external memory, such as writing files on the SD card
READ_SMS	Allow reading SMS content
WRITE_SMS	Allow writing text message
INSTALL_PACKAGES	Allow the program to install applications
MOUNT_UNMOUNT_FILESYSTEM	Allow to mount, anti-mount external file systems
ACCESS_COARSE_LOCATION	Allow users to access the location information through WIFI or mobile base station
INSTALL_SHORTCUT	Allow creating shortcuts

3 Suspicious API

Android API allows applications to access the phone's sensitive data, resources, and send text messages, download applications, etc. With API only, can just determine what kind of behaviors exists in the application, and to analyze whether these behaviors are harmful, you need to continue analyzing the parameters of API calls, such as phone numbers, etc.. Currently the developers use a majority of API provided by Google official to develop applications and few use proprietary API. This paper collects suspicious API of mobile payment applications based on the analysis code of malicious applications provided by Google official SDK and security vendors like Jinshan. Further information shown as follows:

- Send SMS: sendTextMessage() or sendMultipartTextMessage()
- Install external packages: installPackage()
- Receive SMS: addAction()
- Uninstall applications: uninstall()
- Delete SMS: delete()
- Send mail: getTransport() and send()
- Execute external commands: Runtime.exec()
- Network connection: execHttpRequest()

4 Special String

According to the above authority, API can describe application behavior, but can not define whether the behavior is harmful. Therefore, basing on the above evaluation index, this paper adds the special string evaluation index to describe the operation of the application behavior, in order to increase the accuracy of assessment. Through analyzing the characteristic of malicious payment application, this paper mainly collects the following special strings: IP, cell phone number, email address, executable command string like pm uninstall com.qihoo360.mobilesafe.

III. EXPERIMENT SETTINGS

A. Data set

This paper collected 1612 normal samples and 387 malicious samples. These samples were from the official Google Play store, domestic third-party shops and related Android Forum. To extract the evaluation index of samples, we mainly use python language to call detection code of open source software Androguard, analyze samples and extract application features. We found that the average numbers of evaluation indicators appearing in the application are as shown in Table 2. Besides, only parts of the malicious samples have a changed signature information. On application privileges, suspicious API, special string, etc., the calls number of malicious application is obviously more than normal application.

Tab. 2 Sample characteristics statistics

Characteristic	*S1*	*S2*	*S3*	*S4*
Normal Sample	0	7.21	5.13	1.51
Malicious Sample	0.59	11.64	7.68	2.79

B. Establish a training sample

In order to construct an assessment model, you need to do the following procession of assessment indicators. Define evaluation index set S, where the signature information, application permissions, suspicious API, special string subset respectively are S1, S2, S3, S4. Among them, S is the set of S1, S2, S3, S4: S = S1 U S2 U S3 U S4. According to set S, you should define a |S| dimensional vector space where each element is either 0 or 1. An application x will be mapped to a vector h(x). As for the evaluation index Si (i = 1, 2, 3…)of application, if the application detects the evaluation index Si, the value is 1, if not, the value is 0, the specific formula is as follows:

$$h : X \to \{0,1\}^{|S|}, h(x) \mapsto (I(x, S_i))$$

$$I(x, S_i) = \begin{cases} 1 & \text{Application x exists } S_i \text{ feature} \\ 0 & \text{Application x doesn't exists } S_i \text{ feature} \end{cases}$$

C. Parameter Selection

In this paper, we use the SVM classification algorithm C-SVC of LibSVM, and choose the most commonly used radial basis kernel function to achieve the nonlinear mapping of sample characteristics. In

order to get the appropriate parameters, first use step search strategy to select parameters, then use cross-validation method to optimize the aim function, and get the optimum parameters of radial basis kernel function. The optimum parameter of penalty factor C is 500, and the kernel parameter x is 0.03325. In this paper, all the SVM experiments use the above mechanism to select parameters. If not specially described, the two parameters based on the radial basis kernel function use the above values as default values. In addition, use Weka software to complete the experiment of Naïve Bayesian and K neighbor classification algorithm.

D. Experimental results

In this paper, the evaluation criteria are defined as follows:

Definition 1, accuracy indicates the accuracy of classification. The average accuracy rate is defined as the ratio of the number of correct classification application and total number of application.

Table 3 shows that the average accuracy rate of SVM is 96.5%, which is higher than the accuracy of Bayesian algorithm and improved Bayesian algorithm. Compared with K-nearest neighbor classification algorithm based on K-means clustering algorithm, the average accuracy rate of SVM algorithm is slightly high. However, its standard deviation is 0.32%, which is far less than other two methods. This indicates that the method has good stability.

Tab. 3Classification accuracy of different algorithms

Data Mining Method	*Accurate rate/%*	*deviation/%*
NB	67.81	9.20
NB+FCBF	92.30	2.32
NBK	93.70	1.93
NBK+FCBF	94.12	3.60
K-means+KNN	95.20	2.20
SVM	96.50	0.32

IV. DISCUSSION

To establish a good support vector machine classification model, it is also faced with the following problems: First, how to ensure the selection of sample feature space is appropriate. The selection of sample characteristics directly affects the recognition accuracy of classifier. If the selected feature is too small and not enough to describe the sample feature, it will lead to a lower accuracy. While the dimension is too high, it will make the speed of training and classification become slow and reduce efficiency. Second, the selection of kernel function. It directly affects the classification accuracy and computation complexity. Third, feature correlation issues. Traditional SVM algorithm assumes that all the features have the same importance. However if the sample contains weak correlation or even irrelevance features with the target function, it will affect the generalization ability of the classifier to some extent, resulting in low learning accuracy. Therefore, this paper will focus on the changes of support vector machine classification performance under different evaluation index set, kernel function, feature weights.

A. Different Evaluation Index Set

Signature information has a decisive role in determining whether the application has been tampered with. Therefore, under the premise of containing signature information, this paper only considers the impact ofdifferent combinations of application permissions, suspicious API, and special strings on the accuracy of evaluation model. Specific results are as table 4. It is difficult to confirm whether the behavior of application is malicious by the corresponding authority and suspicious API only, so the accuracy rate of combination 1 is the lowest. Although the combination of 2 and 3 are respectively lack of application permissions and suspicious API, we found that the code of normal application would not exist special string in general. As long as there is a special string, can determine whether an application is harmful to a great extent. Thus, the accuracy of 2 and 3 is close or even higher than combination 1. Besides, there are some applications in which the special strings can not be detected and the signature information is invalid at the same time. Under this circumstance, the identification of application relies on authority and suspicious API. Therefore, the classification performance is best only when the four features are integrated.

Tab. 4The experimental results of different evaluation sets

Serial Number	*Feature Combination*	*Accurate Rate/%*	*Training Time/s*
1	S1+S2+S3	91.10	206
2	S1+S2+S4	93.35	156
3	S1+S3+S4	93.66	280
4	S1+S2+S3+S4	96.50	300

B. Different Kernel Function

In the third part of this article, we choose the radial basis kernel function for modeling. This modeling can not guarantee the best performance of the model. Therefore, we need to discuss the accuracy of linear kernel, polynomial kernel and radial basis kernel classification, so as to choose the best kernel function. The experimental results are as shown in table 5, the linear kernel function is simple and its performance is the worst. The polynomial kernel function belongs to the global kernel function. It has global characteristics and allows data points which are far apart to have impact on the value of kernel function. Therefore, the polynomial kernel function is suitable for the independent distribution of features in this article and has best performance. Radial basis kernel function, has complex training process, and stressed the local nature of sample, the stability is also worse than polynomial kernel function. Taking all these into consideration, the support vector machine based on polynomial kernel function is optimal.

Tab. 5The experimental results of different kernel functions

Kernel Function	*Accurate Rate/%*	*Training Time/s*
Linear	95.03± 2.09	577
Polynomial	96.99± 0.12	450
Radial Basis	96.50± 0.32	300

C. Different Feature Weights

Different characteristic items S_1, S_2, S_3, S_4 have different degree of impact on the category of mobile payment application. According to the characteristics of each evaluation index, we compare the accuracy of classification model based on polynomial kernel function under three sets of feature weights W_1 = (0.3151, 0.2223, 0.2030, 0.2596), W_2 = (0.2231, 0.3026, 0.2706, 0.2037), W_3 = (0.4063, 0.1499, 0.1368, 0.3070) by pairwise comparisons. From table 6, it can be found that if the design of weight is not reasonable, it will lead to a lower accuracy rate of detection. For example, the weight W_2 reduces the importance of signature information and special string, resulting in a dropping accurate rate. In weight W_2 and W_3, the signature information as main attribute, special strings as secondary attributes, weaken the impact of authority and suspicious API on classification, and improve its accuracy. However, the weights of authority and suspicious API are too small in W_3, resulting in partial signature information has not been changed and special strings can not be extracted. This causes that some malicious applications are judged to be normal application, and gets a lower accuracy than W_1.

Tab. 6 The experimental results of different feature weights

Serial Number	*Feature Wight*	*Accurate Rate/%*
1	W1	97.82
2	W2	94.16
3	W3	97.21

V. CONCLUSION

In this paper, we study the security assessment issue of mobile payment application based on support vector machine (SVM). By comparing SVM algorithm, Naive Bayesian and its improved algorithms, K nearest neighbor classification algorithm, the experiment proves that the performance of SVM is the best, and its accurate rate is 96.5%. Through further optimizing evaluation performance, discussing the impact of

different evaluation index sets, kernel functions, feature weights on SVM performance, it turned out that the feature set used in paper is better, and the polynomial kernel function can get better classification performance. In addition, by introducing feature weights, it will better balance the importance of evaluation index in sample classification, and increase the classification accuracy to 97.82%. In order to distinguish whether an application is malicious more accurately, the following aspects should be taken into consideration in future work: First, introduce sample weight to reduce the negative impact brought by the uneven sample data. Second, with the emergence of new malicious sample, new evaluation index can be introduced to avoid the decrease of accuracy caused by insufficient index.

REFERENCES

[1] Cao Wei, Zhao Yan. A security technology research of mobile payment based on two factor authentication[J]. In: Information Security and Technology, 2014, 5(2):10-12.

[2] Wei Hongchun, Ma Ding. Mobile payment security solution based on improved secure 3-D protocol[J]. In: Computer application and software, 2011, 28(4): 189-192.

[3] Shi Tengfei, Cheng Linjing, Zhang Ying, etc. Design and implementation of WAP security mobile payment system based on Android[J]. In: Information Network Security, 2012, 11:014.

[4] Peng H, Gates C, Sarma B, et al . Using probabilistic generative models for ranking risks of android apps [A]. In: Proceeding of the 2012 ACM conference on Computer and communications security[C]. ACM, 2012: 241-252.

[5] Wu D J, Mao C H, Wei T E, et al. Droidmat: Android malware detection through manifest and API calls tracing[A]. In: Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on[C]. IEEE, 2012:62-69.

[6] Barrera D, Kayacik H G, van Oorschot P C, et al. Amethodology for empirical analysis of permission-based security models and its application to android[A]. In: Proceeding of the 17th ACM conference on Computer and communications security[C]. ACM, 2010:73-84.

[7] Hu Wenjun, Zhao Shuang, Tao Jing, et al. Detection method and system implementation of malicious code for Android platform[J]. In: Journal of Xi'an Jiao Tong University, 2013, 47 (10): 37-43.

[8] Sarma B P, Li N, Gates C, et al. Android permissions: a perspective combining risks and benefits[A]. In: Proceedings of the 17th ACM symposium on Access Control Models and Technologies[C]. ACM, 2012:13-22.