Digital Evidence Evaluation System Based on Computer System Environment Analysis

Gonglong Chen
Department of Computer Science and Technology
East China University of Political Science and Law
Shanghai, China
cgl1428719317@163.com

***Abstract*—In cybercrime, the evaluation results of the weight of digital evidence are directly influencing the cognizance of the relevant case, further influencing the judgment of the case. Now, it lacks a universally accepted standard to evaluate the weight of digital evidence. Furthermore, the result of the evaluation will be easily influenced by experts. A system, which is based on Naive Bayesian Classification, of digital evidence evaluation is put forward in this paper. It can help normalize the evaluation process effectively and automatically, avoid manual intervention, and then provide reliable evaluation results for the judge's judgment.**

Keywords—digital evidence; evidence evaluation; Naive Bayesian Classification

I. INTRODUCTION

The advent of the Internet era brings us a lot of convenience, but the disputes on network transaction and cybercrime are also increasing. This requires lawful and adequate, effective and persuasive digital evidence to provide support.

In other words, digital evidence must have sufficient admissibility before it could become the evidence that a judge can rely on. The admissibility, which is closely related to legitimacy, relevance and authenticity, refers to whether a material evidence can be shown as an evidence in court. Legitimacy refers to the form, the evidence collection procedures or extraction method must be in conformity with law[1]. Relevance refers to the objective relationship between the evidence and the case. Authenticity refers to whether the evidence itself is real. Compared to the traditional evidence, digital evidence may have some unstable factors that make the identification of its authenticity more difficult.

Generally, there are two kinds of method to identify the authenticity of digital evidence: the method of direct identification and the method of indirect identification.

Regarding the direct identification method, it is based on the content of the digital evidence. In Chinese legislation, only after the material passing a verification can it be used as the evidence to determine facts. Nevertheless, this method is not applicable for the digital evidence, since the digital evidence is easy to be modified.

With reference to the indirect identification method, it is according to the reliability of the computer system, which involves whether there is a trace of malicious behavior, whether it has been hacked or whether there are residues of malicious software in it.

In short, digital evidence should have authenticity, reliability and integrity. For the cognizance of authenticity of digital evidence, the court often requires the center of judicial expertise to identify the evidence. The results of evaluation usually depend on the personal experience of experts, lacking a unified evaluation standard. Therefore, it is difficult to guarantee the justice, consistency and reliability in the process of digital evidence evaluation. To compensate for the deficiencies of the artificial evaluation, many methods like statistics and artificial intelligence have been applied to the field.

For example, in the field of DNA analysis, people begin to apply data mining methods into analyzing DNA sequences. At first, DNA sequence data is mapped to a suitable form. And then generic algorithms are used to mine DNA sequence data. There are many common algorithms like sequential pattern mining method based on prefix projection[2-6], K-medoid based on divide[7], single-link based on gradation[8], Decision Tree[9], Neural Networks[10], Support Vector Machine[11] and so on.

Data mining is a common technique, it can also evaluate the authenticity of the digital evidence. From the perspective of the characteristics of digital evidence evaluation, how to design the algorithm is the key problem.

Naive Bayes algorithm is now recognized as a simple and effective method for probabilistic classification. It is a simplified Bayesian, which assumed that there are no links between the various factors.

As a simple and efficient classification, Naive Bayesian Classification has been successfully applied in various fields like intrusion detection, weather forecasting, spam-email filtering and so on.

For example, in the spam email filtering, according to the training set, Naive Bayesian Classification can be used for training automatically. And the results reflect the nature of the training set. Therefore, users can provide a certain number of

This paper was sponsored by the Creative Activity Plan for Shanghai University Students (201310276106).

978-1-4799-2030-3 /14/$31.00 ©2014 IEEE

e-mail spam and non-spam to train their filter for spam filtering[12].

This article, firstly, makes a brief introduction to the Naive Bayesian Classification algorithm. Then it designs a digital evidence evaluation model based on Naive Bayesian Classification algorithm. Accordingly，it uses samples to test the evaluation model. Finally, it summarizes the evaluation model.

II. THE METHOD OF DIGITAL EVIDENCE EVALUATION

A. The Brief Of Naive Bayesian Classification

In (1), $\{a_1, a_2, \ldots\ldots, a_n\}$ on behalf of n-dimensional feature vectors, each a for an attribute of x [13].

$$x = \{a_1, a_2, \ldots\ldots, a_n\} \tag{1}$$

Assume a category $C = \{y_1, y_2, \ldots\ldots, y_m\}$, given an unknown sample data x, calculating the value of each vector respectively in (2).

$$P(y_1|x), P(y_2|x), \ldots\ldots, P(y_m|x) \tag{2}$$

Among them, $P(y_m|x)$ refers to the incidence of the y_m under the condition of x.

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)} \tag{3}$$

By the theorem of Bayes in (3), at the same time, assume that each feature attribute of each data sample is conditional independence, then we can get (4) [14].

$$P(x|y_i)P(y_i) = P(y_i)\prod_{j=1}^{n} P(a_j|y_i) \tag{4}$$

Where $P(y_i)$ is the prior probability of y_i, prior probability can be obtained with $P(y_i) = S_i/S$, S_i that belongs to y_i is the number of training samples, S is the sum of training samples[15].

Under the circumstances that each attribute of the data sample is conditional independence, the method to get $P(x|y_i)$ is different according to the discrete and continuous attributes.

When the feature attributes are discrete, just by counting the frequency of each internal of the training samples in each category, you can estimate $P(a_j|y_i)$ in (5).

$$P(a_j|y_i) = S_{kj}/S_i \tag{5}$$

S_{kj} is the number of the training sample of the category y_i on the attribute a_j, and S_i is the number of the training sample in category y_i.

When the feature attributes are continuous, we assume that attributes to obey Gaussian distribution, and then get (6).

$$P(a_j|y_i) = G(a_j, \eta_{yi}, \sigma_{yi}) \tag{6}$$

Thus, calculating the mean and standard deviation of each internal of the training samples of each category, and generating them into the formula[16-17].

$$P(y_k|x) = \max\{P(y_1|x), P(y_2|x), \ldots\ldots, P(y_m|x)\} \tag{7}$$

Finally, X belongs to the classification which corresponds to the largest value of $P(y_k|x)$ in (7).

B. The Design Of Naive Bayesian Classification

Set the feature attributes of the samples. *PORT* represents the ratio of malicious connecting ports. *PROCESS* represents the ratio of malicious running processes. *ACCESS* represents whether access control rules have been added. Each attribute has their own internal.

They are shown in the TABLE I.

TABLE I. FEATURE INTERNALS

Feature Name	Internal 1	Internal 2	Internal 3
PORT	0~PLEVELA	PLEVELA ~PLEVELB	PLEVELB~1
PROCESS	0~ PLEVELA	PRLEVELA ~PRLEVELB	PRLEVELB~1
ACCESS	TRUE	FALSE	-

PLEVELA, *PLEVELB* and *PRLEVELA*, *PRLEVELB* represent the critical values of *PORT* and *PROCESS* (sampled from the database). *TRUE* means access control rule has been added. *FALSE* is opposite.

Set the class aggregation, *C = {RELIABLE, UNRELIABLE}*. *RELIABLE* represents that this attribute is reliable. *UNRELIABLE* represents that this attribute is unreliable. Get the number of two kinds of computer from the database. The number of reliable computers: *MRE*. The number of unreliable computers: *MUNRE*. So,

$$P(RELIABLE) = MRE / (MRE + MUNRE) \tag{8}$$

$$P(UNRELIABLE) = MUNRE / (MRE + MUNRE) \tag{9}$$

Then calculating the frequency of each attribute in their internal separately, according to the method mentioned in Naive Bayesian Classification.

The example is shown in the TABLE II.

TABLE II. A SECTION PROBABILITY EXAMPLE

Section	Probability of Each Section
Reliable Port	P(PORT < PLEVELA) = P_R_PORTIONA
	P(PLEVELA < PORT < PLEVELB) = P_R_PORTIONAB
	P(PORT > PLEVELB) = P_R_PORTIONB
Unreliable Port	P(PORT < PLEVELA) = P_U_PORTIONA
	P(PLEVELA < PORT < PLEVELB) = P_U_PORTIONAB
	P(PORT > PLEVELB) = P_U_PORTIONB
Reliable Process	P(PROCESS < PRLEVELA) = PR_R_PORTIONA
	P(PRLEVELA < PROCESS < PRLEVELB) = PR_R_PORTIONAB
	P(PROCESS > PRLEVELB) = PR_R_PORTIONB
Unreliable Process	P(PROCESS < PRLEVELA) = PR_U_PORTIONA
	P(PRLEVELA < PROCESS < PRLEVELB) = PR_U_PORTIONAB
	P(PROCESS > PRLEVELB) = PR_U_PORTIONB
Reliable Access	P(ACCESS = TRUE) = A_R_PORTIONT
	P(ACCESS = FALSE) = A_R_PORTIONF
Unreliable Access	P(ACCESS = TRUE) = A_U_PORTIONT
	P(ACCESS = FALSE) = A_U_PORTIONF

After that, just feeding the value of each feature attribute of Sample x into calculation. For example,

$$P(C = RELIABLE|x) = P(C = RELIABLE) * P(x|C = RELIABLE) \quad (10)$$

Then the result of *PROBABILITY_RE* is (11)

$$MRE/(MRE + MUNRE) * P\_R\_PORTIONA * PR\_R\_PORTIONAB * A\_R\_PORTIONT \quad (11)$$

On the other hand,

$$P(C = UNRELIABLE|x) = P(C = UNRELIABLE) * P(x|C = UNRELIABLE) \quad (12)$$

Then the result of *PROBABILITY_ UNRE* is (13)

$$MUNRE/(MRE + MUNRE) * P\_U\_PORTIONA * PR\_U\_PORTIONAB * A\_U\_PORTIONT \quad (13)$$

Through comparing the value of *PROBABILITY_RE* and *PROBABILITY_UNRE*, we can know which side (reliable or unreliable) the Sample X belongs to.

III. TEST THE CLASSIFICATION

The main functions have been realized by computer software. The continuous attributes consist of malicious process ratio (PR), malicious port ratio (PT), malicious automatic run software ratio (AR).The discrete attributes consist of the firewall open status (FW), the Anti-virus software installed status (AV), the "host" file's status (HT), the file extension name modified status (ET). The samples used for testing and training are all from laboratory. Of course, the reliability is known and the feature attribute is given. According to the "Control Variables Method", half of the samples are used to train classification and the rest are for testing.

The testing result after using classification is shown in TABLE III.

TABLE III. RATIO OF EVALUATION

	Reliable ratio	Unreliable ratio
Classification	60%	40%
Reality	51%	49%
Deviation	9%	9%

The system has a good evaluating ability, which can be seen from the result. But, some parts can also be improved like how to adapt to the changeable environment, how to build a stronger classification.

IV. CONCLUSIONS

In conclusion, there are three major characteristics in the system.

Firstly, this system adopts a method named Naive Bayesian Classification, which is now recognized as a simple and effective probability classification method. Its simple structure, small computational complexity and high classification accuracy, can improve the efficiency of modeling[18-22]. It can also overcome the low efficiency in modeling and the difficulty in implement of the Decision Tree[23-24] and the structure of the Support Vector Machine (SVM)[25].At the same time, as a kind of probability classification model, its probability of each attribute conditional has clear physical meaning and good interpretability, which can overcome the difficulty in explaining Neural Network Classification[26].

Secondly, the evaluation system is based on the computer overall environment and the digital evidence itself. Comprehensive evaluation of the property can draw a more reliable evaluation result.

Thirdly, this system is implemented as a computer software based on a computing model, which will generate result according to the digital evidence, hence it can get over the defects of the subjectivity and the instability in expert's evaluating process, thus making the evaluation process more objective and reliable.

With the help of Naive Bayesian Classification, the system provides an effective measure of evaluating digital evidence. It avoids the artificial interference and takes a good use of Bayesian Classification's feature to deal with great amounts of data. Thus, a reliable result of digital evidence's probative force can be given to help judges make their judgment.

ACKNOWLEDGMENT

We would like to acknowledge the support of the Creative Activity Plan for Shanghai University Students (201310276106) in this work.

REFERENCES

[1] He Jiahong, A new course in evidence law, Lawpress China, 2000,p.109

[2] Agrawal R., Srikant R., "Mining sequential patterns," in Yu PS, Chen ALP, eds. Proc. of the 11th Int'l Conf. On Data Engineering. Taipei: IEEE Computer Society, 1995, pp.3-14

[3] Srikant R., Agrawal R., "Mining sequential paterns: generalization and performance improvements," in APers PMG, Bouzeghoub M., Gardarin G, eds. Advances in Database Technology, Proc. of the 15th Int'l Conf. on Extending Database Technology. London: Springer-Verlag, 1996, pp. 1-17

[4] Pei J., Han J.W., Mortazavi-Asl B., Pinto H.Prefixspan, "Mining sequential patterns efficiently by prefix-projected growth," in Proc. of the 17th Int'l Conf. on Data Engineering. Washington: IEEE Computer Society, 2001, pp. 215-224

[5] Han J., Pei J., Mortazavi-Asl B., Chen Q.M., Dayal U., Hsu MC.Freespan, "Frequent pattern-projected sequential pattern mining," in Proc. of the 6th ACM SIGKDD Int'l Conf. on Knowledge Discovery in Databases. New York: ACM, 2000, pp.355-359

[6] Zaki M.J., "SPADE: An efficient algorithm for mining frequent sequences," Machine Learning, 2001, 42(1-2), pp.31-60

[7] Kaufman L., Rousseeuw P.J., Finding Groups in Data: An Introduction to Cluster Analysis, New York: Johh Wiley&Sons, 1990

[8] Day W.H.E., Edelsbrunner H., "Efficient algorithms for agglomerative hierarchical clustering methods," Journal of Classification, 1984,1(1), pp.7-24

[9] Quinlan J.R., C4.5: Programs for Machine Learning, San Francisco: Morgan Kaufmann Publishers, 1993

[10] Ripley B.D., Pattern Recognition and Neural Networks, Cambridge: Cambridge University Press, 1996

[11] Vapnik V.N., The Nature of Statistical Learning Theory, 2nd ed., New York: Springer-Verlag, 2000, pp.138-167

[12] Wei Zheng,"Implementing Span Filter by Improving Navie Bayesian Algori -thm,"Journal of Northwestern Polytechnical University,Aug 2010,Vol 28 NO.4 pp.622-627

[13] Gong Xiujun, "Research on Bayesian Learning Theory and its Application," Bei Jing: Institute of Computing Technology Chinese Academy of Sciences, 2002, pp.24-25

[14] Langley P., Iba W., Thompson K., "An analysis of Bayesian classifiers," Proc. of the10th National Conference on Artificial Intelligence. 1992

[15] Harry Z., Sheng S.L., "Learning Weighted Naive Bayes with Accurate Ranking," Fourth IEEE International Conference on Data Mining(ICDM'04). 2004

[16] Chickering D. M., Learning Bayesian networks is NP-complete, Learning from Data: Artificial Intelligence and Statistics. 1996

[17] Zhang Jun, "An algorithm for learning compact and accurate naive Bayes classifiers from attribute value taxonomies and data," Fourth IEEE International Conference on Data Mining(ICDM'04). 2004, pp.289-296

[18] Langley P., Sage S., "Induction of selective Bayesian classifier," Proceedings of the 10th Conference on Uncertainty in Artificial Intelligence. 1994

[19] Kononerko I., "Semi-naive Bayesian Classifiers," in Proceedings of European Conference on Artificial Intelligence. Porto, Portugal: Springer-Verlag, 1991, pp.206-219

[20] Han J., Micheline K., Data mining concepts and techniques. Chicago: Morgan Kaufmann Publishers, 2000

[21] Domingos P., Pazzani M., "On the optimality of the simple Bayesian classifier under zero-one loss," Machine Learning, 1997, 29(2-3), pp.103 -130

[22] Friedman N., Yakhini Z., "On the sample complexity of learning Bayesian networks," Proceedings of the 12th Conference on Uncertainty in Artificial Intelligence. 1996

[23] Safavian, S.R., "A survey of decision tree classifier methodology," IEEE Transactions on Man and Cybernetics, 1991, pp.660-674

[24] Friedl M.A., Brodley C.E., "Decision tree classification of land cover from remotely sensed data," Remote Sensing of Environment, 1997, pp. 399-409

[25] Schuldt, C., Laptev I., Caputo B., "Recognizing human actions: a local SVM approach," Proceedings of the 17th International Conference on Pattern Recognition, 2004

[26] Odom M. D., Sharda R., "A neural network model for bankruptcy," in IEEE International Joint Conference on Neural Networks, SanDiego, California, 1990, 2(7), pp.163-168