Study on Attribute Reduction Method of Network Intrusion Detection System Based on Granular Computing

Leng Tianyi
International School
Beijing University of Posts and Telecommunications
Beijing, China
lengtianyi@bupt.edu.cn

Li Haiyan
School of Science
University of Science and Technology Liaoning
Anshan, China
lhyqmj@163.com

***Abstract*—Based on granular computing theory, according to the problem of intrusion detection classification performance reduced by redundant attribute in high dimensional network data, an attribute reduction method of network intrusion detection system based on granular computing is given, the redundant attribute is removed under the condition of keeping the information integrity of original attribute set to reduce the attribute dimension of data. The example analysis indicates that this method reduces the training and detection time, and improves the computing efficiency of system in order to reduce the data storage, it provides a new idea for processing massive large data.**

Keywords- granular computing; network intrusion detection system; attribute reduction

I. INTRODUCTION

With the development of computer network and information technology, the network security is a series problem. The traditional network security technology such as firewall, access control mechanism and data encryption are attacked by hacker, therefore, the intrusion detection system becomes a hot and important research direction of network security. The intrusion detection system is a second safe gate for network defense system. However, there are large amount of audit data for a small network, the classification of intrusion detection becomes very difficult due to the existing redundant information, hence how to improve the system efficiency, system accuracy and reducing the data amount are the important problems in real time intrusion detection [1].

The redundant information comes from the redundant attribute and redundant attribute value, the data reduction consist of attribute reduction and attribute value reduction. The objective of attribute reduction [2-3] is to obtain a reduction attribute set and keep the information integrity of original attribute set to reduce the attribute dimension of data and remove the redundant attribute. The attribute value reduction simplifies the data set on the basis of attribute selection to remove the redundant value of rest attributes.

According to the granular computing theory [4-5], each attribute has the indiscernibility relation in multi-dimensional qualitative attribute, however not every attribute will affect the object classification, the importance of attribute is taken as the standard of attribute selection, the attribute core is start point, the redundant attributes are selected by defining the importance of attribute to realize the attribute reduction. This attribute reduction algorithm can process a large amount of data, and improve the network efficiency, the example analysis proves its effectiveness and feasibility.

II. RELATIVE CONCEPT AND SYMBOL DESCRIPTION OF GRANULAR COMPUTING

Normally, $S=(U,A,V,f)$ denotes an information system, where U denotes non empty set of observed object, which is called discourse domain; A denotes non empty set of attribute; $V=\bigcup\{V_a \mid a\in A\}$, V_a is the range of attribute a; $f:U\times A\to V$ is an information function, it assigns an information value for each attribute, thus $a\in A$, $x\in U$, hence $f(x,a)\in V_a$.

Specially, if the attribute set of observed object is $A=C\bigcup D$, where C and D are condition attribute set and decision attribute set respectively, which satisfy $C\bigcap D=\varnothing$, and $D\neq\varnothing$, then the information system S is called a decision system.

The particle is an initial concept of granular computing, it is a unit of research object. The size of particle is measured by particle size, which is different by different angles. From the viewpoint of information theory, the size of particle can be measured by amount of information in it.

Let attribute subset be $P\subseteq A$, the division of P on U is:

$$U/P=\{[x]_P \mid x\in U\}=\{x_1,x_2,\cdots,x_n\}$$

Define the information particle P is:

$$GD(P)=\sum_{i=1}^{n}\left|X_i\right|^2/\left|U\right|^2$$

where $\sum_{i=1}^{n}\left|X_i\right|^2=1$ is a cardinal number of equivalent relation determined by attribute subset P.

By using the definition of attribute particle size [6], the importance of each attribute can be analyzed in multi-dimensional qualitative attribute. Assume that a is an attribute in attribute set A, then if a is removed in A, then the attribute particle size will be changed. For the importance of A, the bigger change is, the more important

a will be. Therefore, the importance of a in A is defined as $Sig_{A-\{a\}}(a)$, $Sig_{A-\{a\}}(a)=GD(A)/GD(A-\{a\})$. If and only if $(GD(A)/GD(A\_\{a\}))\neq 1$, a is a core attribute of A, hence the core of A can be denoted as:

$$Core(A)=\left\{a\in A \mid Sig_{A-\{a\}}(a)<1\right\}.$$

The defined importance of attribute is taken as a standard of attribute selection, the attribute core is start point, a reduction set of multi-dimension qualitative attribute [7].

III. Attribute Reduction of Network Intrusion Detection System Based on Granular Computing

The data set of network flow rate can be seen as a special information system $T=(U,A,V,f)$, where $U=\{x_1,x_2,\cdots,x_m\}$ is a set of network flow rate sample, $A=\{a_1,a_2,\cdots,a_n\}$ is an attack attribute set, is a set of attribute values.

According to the particle view [8], each attribute in information system has a certain resolution, therefore, each attribute has its own particle size, they are converged together to generate a stronger attribute set. The defined importance of attribute is taken as a standard of attribute selection, the attribute core is start point, the attribute is increased on the basis of attribute core until obtaining the reduction set of attack attribute set.

Basic steps of attribute reduction algorithm:

Step 1, calculate attribute core $Core(A)$

Firstly, calculate the particle size $GD(A)$ of attribute A, then remove any attribute a, and observe whether the particle size of rest attributes changes or not, if changes, then the attribute a is a core attribute, otherwise it is not a core attribute, $Core(A)$ may be an empty set, and let $Red(A)=Core(A)$.

Step 2, determine division of attribute set A and $Red(A)$ on U, and judge whether they are equal or not

If they are equal, then $Red(A)$ is a reduction set; if not, then calculate all importance $Sig_{Red(A)}(a_i)$ of $a_i\in A-Red(A)$, attribute a_1 is selected to satisfy $Sig_{Red(A)}(a_1)=\max\limits_{a\in A-Red(A)}\left\{Sig_{Red(A)}(a)\right\}$, and a new reduction set $Red(A)=Core(A)\cup\{a_1\}$ is generated.

Step 3, repeat step 2 until obtaining the reduction set of attributes.

The flow chart is shown in figure 1.

IV. Example Analysis

KDDCUP1999 data sets are adopted, each sample consists of basic attribute set, concept attribute set, time attribute set and host computer attribute set. There are 41 attributes, which are including 9 discrete attributes and 32 continuous attributes. There are many modes in network attacking, here 4 main kinds modes, i. e. DOS, Probe, R2L and U2R are chose to test.

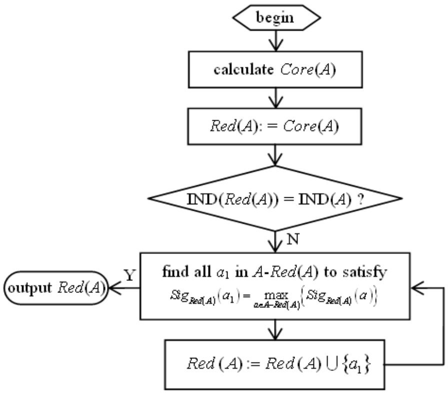
begin
calculate $Core(A)$
$Red(A) := Core(A)$
$IND(Red(A)) = IND(A)$?
N
Y
find all a_1 in A-$Red(A)$ to satisfy
$Sig_{Red(A)}(a_1)=\max\limits_{a\in A-Red(A)}\{Sig_{Red(A)}(a)\}$
output $Red(A)$
$Red(A) := Red(A)\cup\{a_1\}$

Figure 1. Flow chart of attribute reduction algorithm

Firstly, a discrete process is carried out for the training sample set and testing sample set, and the experiment data set is obtained in table I and table II.

TABLE I. Experiment Data set: Training Sample Set

attack mode	training sample set (number)		
	sample	*normal sample*	*attack sample*
Dos	12967	9764	3203
Probe	7551	6631	920
R2L	5840	5157	683
U2R	1378	1358	20

TABLE II. Experiment Data set: Test Sample Set

attack mode	test sample set (number)		
	sample	*normal sample*	*attack sample*
Dos	2596	1953	643
Probe	1512	1327	185
R2L	1171	1034	137
U2R	692	679	13

By using the attribute reduction algorithm, a reduction is carried out for experiment data in table I, and an optimal attribute subset of network data are obtained, showed in table III.

TABLE III. Optimal Attribute Subset After Reduction

attack mode	optimal attribute subset of network data
Dos	protocol-type, service, dst-bytes, flag
Probe	src-bytes, dst-bytes, flag, srv-count, dst-host-same-srv-count
R2L	service, dst-bytes, dst-host-srv-count
U2R	duration, service, dst-bytes, dst-host-count

From table III, it is easy to see that the numbers of attribute sets is decreased by using the attribute reduction algorithm in four attack modes, specially in R2L attack mode, the numbers of attribute sets is decreased from 41 to 3, the reduction rate is 92.68%.

In order to test the effectiveness of this algorithm, SVM is used as classification detection algorithm, a SVM training is carried out for sample sets, and the detection results are shown in table IV and table V.

TABLE IV. SVM DETECTION RESULTS BEFORE REDUCTION

attack mode	attribute number	training time/s	detection time/s	detection rate (%)	false alarm rate (%)
Dos	41	4.546	1.594	99.89	0.01
Probe	41	1.735	0.625	96.24	0.35
R2L	41	1.687	0.568	52.17	0.45
U2R	41	0.313	0.281	50.00	0.37

TABLE V. SVM DETECTION RESULTS AFTER REDUCTION

attack mode	attribute number	training time/s	detection time/s	detection rate (%)	false alarm rate (%)
Dos	4	1.271	0.240	100.00	0.00
Probe	5	0.776	0.165	100.00	0.03
R2L	3	0.643	0.163	91.98	0.05
U2R	4	0.013	0.014	91.65	0.10

By comparing table 4 with table 5, it is easy to see that SVM algorithm reduce the training and detection time in four attack detections after the attribute reduction algorithm, specially in Dos attack detection, the training time and detection time is reduced by 71.82% and 84.32% respectively. Simultaneously, the detection rates of four attack detections are improved obviously and it keeps a low false alarm rate, specially in R2L and U2R attack detection, the detection rates of them are improved by 78.19% and 83.34% respectively, and the false alarm rate keeps a low level between 0 to 3.25%.

REFERENCES

[1] X. D. Xu, Y. Gu, and S. R. Zhu, “Research on data reduction in intrusion detection,” Computer Engineering, vol. 37, no. 11, pp.170-172, June 2011.

[2] W. X. Zhang and G. F. Qiu Uncertain Decision Making Based on Rough Sets, Tsinghua University Press, 2006.

[3] Y. Gu, T. J. Zhang, J. Fan and L. He, “Intrusion detection basing on concept lattice,” Journal of Huazhong University of Science and Technology, vol. 31, no. s1, pp. 156-158, 2003

[4] X. H. Li and K. Q. Shi, “A knowledge granulation-based algorithm for attribute reduction,” Journal of Computer Applications, vol. 26, no. Z1, pp. 76-78, June, 2006.

[5] J. Y. Wu, “The application of rough set attribute reduction in intrusion detection system,” Journal of Changsha University, vol. 24. no. 2, pp. 47-49, Mar, 2010.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

V. CONCLUSION

In this paper, in order to solve the problem of intrusion detection classification performance reduced by redundant attribute in high dimensional network data, an attribute reduction method of network intrusion detection system based on granular computing is proposed. A data reduction is carried out by using high dimensional data in KDDCUP1999 to verify the feasibility of this algorithm, the results show that this algorithm can reduce the attributes of high dimensional network data effectively, simplify the training and detection data set, reduce the training and detection time, save the storage resource and improve the intrusion detection classification performance.

ACKNOWLEDGMENT

The work was supported by Natural Science Foundation of Liaoning Province under Grand 20102097.

Corresponding author: Li Haiyan, lhyqmj@163.com.

[6] Z. Mo and H. Lin, “Knowledge reduction algorithm based on granular computing,” Computer Science, vol. 36, no. 8A, pp. 237-241, 2009

[7] H. Ding, S. F. Ding and L. H. Hu, “Research progress of attribute reduction based on rough sets,” Computer Engineering & Science, vol. 32, no. 6, pp. 92-94, 2010.

[8] L. P. Guo, J. C. Xu, H. L. Meng and J. L. Shi, “A new attribute reduction algorithm based on knowledge granulation,” Computer Science, vol. 34, no. 8A, pp. 146-148, 2007.

[9] A. Hamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[10] F. Deng and H. Pan, “Research of intrusion detection system model based on granular computing,” Modern Electronics Technique, vol. 34, no. 10, pp. 115-117, May, 2011.