Mail Detection Model of Campus Network Based on the Adaptive Learning Algorithm

Bin Chen, Yizhou Dong, and Mingrong Mao

***Abstract*—Concerning the problem that a large number of spam disturbing the user, a method named adaptive learning algorithm was proposed. The passive attack method based on the Simple Mail Transfer Protocol(SMTP) session log initiated by the mail host in the campus during half a year. Analysis on the status of delivery rate and many types of failure message of the host behavior in the session record, and ultimately achieve effective adaptation by detecting spam source host behavior on the recent email classification. The experimental results show that the implementation of a number of rounds of classification strategy adjustment, at last the detection accuracy can reach 94.7%. The design is very useful for network administrators, he can effectively detect spam internal host status, and control the behavior of the spam host in the beginning.**

***Index Terms*—Spam host, SMTP session, adaptive learning, categorizer, failure information.**

I. Introduction

Authoritative survey report shows that more than 90% of the total Internet email is spam [1], which is a waste of storage space and bandwidth of the Internet mail service provider. What is more, the senders of spam by sending malicious software embedded spam, or contain harmful drive link to download the type of attack, the lack of immunity of the host becomes a zombie controlled Botnet, forcing it as the effective distribution of spam [2]. To solve this problem the most common strategy is to maximize user filtering from external spam, its actual effect depends on the mail service provider, the client or the ability to filter mail agent provided by mail [3]. Even if the terminal filter can accurately isolate spam, but it still cannot be sent from the source to curb spam, so a lot of network bandwidth will be endless consumption, which will undoubtedly make the already tight campus network bandwidth one disaster after another. Therefore, how to stop spam from the source has become an urgent and important issue in the field. This article from the angle of external mail server and message categorizer operation details view, describes the behaviour characteristics of the corresponding case of spam message multiple failure, an important feature of each host is spam detection after the deep learning. At the same time, a bulking inactive attack adaptation arithmetic is used to monitor the spam host from a large number of SMTP record. The model contributes to the managers of the campus network to detect spam hosts, and thus inhibit the behaviour of these hosts, of course, this method is also applicable to other institutions and scenarios.

Manuscript received February 13, 2017; revised April 12, 2017.

The authors are with Nanjing Normal University, Jiangsu, China (e-mail: 60167@njnu.edu.cn)

II. Research Background

The reason why take spam host detection as the focus of research is that the botnet detection and its correlation is low. In 2012, researchers have made a tentative study on the output message received by the university campus spam filter. The experiment uses a sequential test to detect the probability that the internal host will continue to send spam. The work does not depend on the external spam filter, which depends mainly on the following two factors: 1) A SMTP session maybe failure because of problems in negotiation process, and if a session in the interactive stage continued failure state, the server will send a spam message, in this case cannot filtering toward the content. 2) A user can automatically forward configuration to the mail server configuration, which will also lead to spam messages received by the repeater, for the specific external accounts of a user, the spam checker will discover spam information from the storage, this judgment can be obtained following the detection results more clearly.

For bulking adaptation and online matching, mass data analysis request appeared in part of the application, including the network transaction analysis, anonymous testing, and interference detection, applications require periodic adaptation of recent data classification [4]. In the same way, spam host classification detection is necessary for identifying recent spam behavior from the SMTP log [5]. Most of the adaptive learning methods are based on decision trees, neural networks, and vector machines.

In order to combat the classification task of the categorizer, the attacker will try to avoid the detection. For an attacker, spammers cannot modify the external server's reply message, which limits its control over the message, so the use of attack learning is minimal. The main work of this paper will focus on the adaptive detection of spam which keeps changing its behaviour.

III. Spam Behavior Characteristics Analysis and Detection Model

The analysis and detection of spam behavior failure message is divided into five stages: 1) The interaction SMTP record is captured by the interference detection system between the inside and outside network of the campus; 2) Extracted The SMTP message from record between the host and the external host in the campus network; 3) Calculate the number and different types of status messages from the internal; 4) In accordance with the host state, through the behavior of the detection method, label the host in the

doi: 10.18178/ijfcc.2017.6.2.490

training set for the internal host normal or abnormal; 5) On this basis, adaptive learning algorithm can be used to continuously detect spam host in Campus. Fig. 1 describes the host computer deployed in the computing center specifically for monitoring SMTP record. The host computer is embedded with a condition monitoring equipment to detect the network status. Network interference detection system analysis by the Key log information collected from the host computer monitoring, in order to carry on the analysis of the SMTP session, which includes the mail address and reply code.

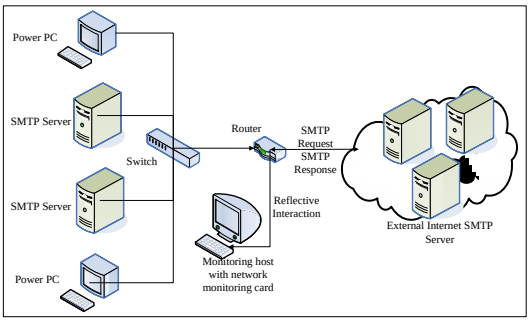

Fig. 1. Computing center host SMTP session monitoring architecture.

When a series of different tagged message arrives, the categorizer need to be constantly updated to keep up with the latest spam behavior matched with the use of this passive aggressive adaptive learning algorithm to adjust to the current categorizer mail samples classification. For each potential sample case, we need to do the following two steps, correct the prediction error of the active categorizer, then update it by active adjustment. Finally, the categorizer which has been minimized after error processing will be used as the categorizer for the next data collection and selection, and then the accuracy of the classification can be improved. The specific labeling of the preceding method needs to be defined prior to its modeling. Labeled periodic data sets P_t are collected during the cycle t . $\{(u_1,v_1),(u_2,v_2),\cdots,(u_{|P^t|},v_{|P^t|})\}$ in the instance array indicate the SMTP behaviour of the host under the condition of eight tuples periodic observation. The corresponding class labels v_n are spam or non-spam identifiers. Set k^t as the weight of the categorizer vector, when each instance $u_n \in P^t$ arrives, the updated categorizer k^{t+1} corrects the error of the previous categorizer k^t . Therefore, it is only to minimize the correctio. If an incorrect prediction value is obtained from k^t by u_n , the adjustment k^t will be replaced by its own boundary value u_n . Set the key (u_n,v_n) as the update model Q based on the k^t .

$$Q(k^t,(u_n,v_n),P^t)=\arg\min\{\frac{1}{2}\|\bar{k}-k^t\|^2+E_0\sum_{u_m\in P^t,u_m\neq u_K}s(\bar{k},(u_m,v_m))\} \quad (1)$$

Here is a variable E_0 that is used to decide how to control the deviation between categorizer bias and prediction error correction. $s(\bar{k},(u_m,v_m))$ is the critical deviation function.

$$s(\bar{k},(u_m,v_m))=\begin{cases}0 & v(\bar{k}\cdot u_m)\geq 1\\ 1-v_m(\bar{k}\cdot u_m) & v(\bar{k}\cdot u_m)<1\end{cases} \quad (2)$$

When the corresponding categorizer of k^t is updated according to the above formula, $\{Q(k^t,(u_K,v_K),P^t):1\leq n\leq|\boldsymbol{P^t}|\}$ is the key of the alternative group on new categorizer. The adaptive learning algorithm is described in the form of semantic modeling as shown in algorithm 1. Its meaning as follows: In every cycle t , Data set P^t will collect data to update the current categorizer k^t , the SMTP behaviour which predicted label display as wrong will be identified by k^t and P^t in the line 4-5 of algorithm 1. Regard to the behaviour instance $u_n \in P^t$, The current classification k^t is updated as a separate categorizer $\overline{k_n}$, update strategy is carried out in accordance with the above formula. If it is selected and obtained the minimum prediction unit in the line 10 of algorithm 1, ultimately the result will be deduced by line 7-8. In addition, exception to minimizing the categorizer deviation, the previous error is corrected also. It can be expected that the method can be used to identify the cases. which distribution state different to the others.

1) $\text{Initialize}: k^1=(0,0,\ldots,0);$
2) $for\ \ t=1,2,\ldots do$
3) $\text{Re}cpt\_Collect\_data(P^t);$
4) $\text{Pr}edict(\hat{v}_u)=sign(k^t u_n)\quad u_n\in P^t;$
5) $Get\quad P^t=\{u_n\,|\,u_n\in P^t, v_u\neq\hat{v}_u\};$
6) $foreach\ \ u_n\in P^t\ \ do$
7) $\tau_n=\dfrac{1-v_n(k^t\cdot u_n)-v_n u_n\sum\limits_{u_m\in P^t,u_m\neq u_n}v_m u_m}{\|\boldsymbol{u_n}\|^2};$
8) $\overline{k_n}=k^t+\sum\limits_{u_m\in P^t,u_m\neq u_n}v_m u_m+\tau v_n u_n;$
9) end
10) $choose$
11) $k^{t+1}=\arg\sum\limits_{u_m\in P^t}s(k,(u_m,v_m))+\|\boldsymbol{k}-\boldsymbol{k^t}\|;$
12) end

Algorithm 1. Formal semantic modelling of adaptive learning algorithm.

IV. Experiment and Analysis

By experiments, we analysis the effect of adaptive learning algorithm on the accuracy of spam detection and its performance. In the experiment, the categorizer is updated

periodically, and the update period is six hours. categorizer k^t is updated by instance tag key P^t in cycle t. The performance of actual effect in correction of the categorizer error by adaptive learning algorithm in different conditions is difference. At the same time, the difference can be reduced to the greatest extent after the update of the categorizer, which can minimize the error in the selection of the potential categorizer. In order to evaluate the performance of the categorizer, it is necessary to emphasize both the classification effect of spam and non-spam hosts, so the average classification accuracy is calculated by the two categories.

Table I list the experimental data set by month. For each instance, the u_n of the item contains the behavior of the eight-tuple vector described in the analysis model before. Each tag of u_n is marked with spam $(v_n = +1)$ or non-spam $(v_n = -1)$.

TABLE I: CAMPUS NETWORK SPAM HOST STATISTICS FROM 2015.11 TO 2016.04

Sample number	Sample name	Host number	Spam host number	Non-spam host number
1	201511	217	26	191
2	201512	222	31	191
3	201601	206	25	181
4	201602	197	31	166
5	201603	235	40	195
6	201604	192	28	164

TABLE II: DETECTION RESULTS OF ADAPTIVE LEARNING ALGORITHM UNDER DIFFERENT PARAMETERS

adaptive Parameter(E0, E)	P1(%)	P2(%)	P3(%)	P4(%)	P5(%)	P6(%)
(0,1)	72.27	82.24	83.87	83.72	83.72	82.37
(0.25,1)	72.27	82.11	82.74	83.51	82.17	81.69
(0.5,1)	72.27	82.25	83.18	83.41	84.28	78.1
(0.25,0)	72.27	72.42	76.27	76.31	76.32	72.72
(0,0)	72.27	72.27	72.27	72.27	72.27	72.27

TABLE III: DETECTION RESULTS FOR SPAM HOST AND NON-SPAM HOSTS

Adaptive Parameter(E0, E)	P1(%)	P2(%)	P3(%)	P4(%)	P5(%)	P6(%)
(0,1), SPH	53.2	88.7	92.2	94.7	94.7	89.9
(0,1), NSPH	91.3	75.8	75.5	72.8	72.8	74.9
(0.25,1), SPH	53.2	90.1	89.9	92.2	88.1	87.5
(0.25,1), NSPH	91.3	75.1	75.51	74.02	76.2	75.9

In the context of different coefficients E_0 and E, the results of the adaptive learning algorithm for the hybrid mail set are shown in Table II. In the experiment, the effects of various parameter E_0 and E values were tried, some representative results are listed in Table II. According to the regulation effect, most of the classification accuracy is improved by $t = 2$ or $t = 3$ in the case of adaptive learning, adaptive learning algorithm has optimal detection ability when $E = 1$. According to the results, the average sorting accuracy was above 80% from the beginning of the second cycle, and remained at a stable level. In addition, when $E_0 = 0, E = 1$ and $E_0 = 0.25, E = 1$, the accuracy is more stable than $E_0 = 0.5, E = 1$. Regard to the categorizer producer, when a new categorizer is formed, the output error monitor correction weight will be reduced to avoid overfitting problem, the adaptive learning algorithm is used to minimize the moderating effect in this experiment.

The details of the analysis under the condition of different adaptive learning configuration classes was listed in Table III. Primary in cases of $E_0 = 0.25, E = 1$ and $E_0 = 0, E = 1$. As can be seen from the table, the recognition accuracy of non-spam hosts is generally less than 80%, some uncertain hosts are also identified as spam hosts because they receive a failed response. Non-spam hosts may impact the deduction results and reduce the accuracy.

In practice, the situation of similar error recognition has been corrected in the form of white list, therefore, the overall accuracy is significantly improved. The average detection accuracy of the three to four cycles of the spam host is more than 90%. The results of the adjustment and prediction accuracy of the spam host and the non-spam host based on different adaptive learning configurations are shown in Fig. 2.

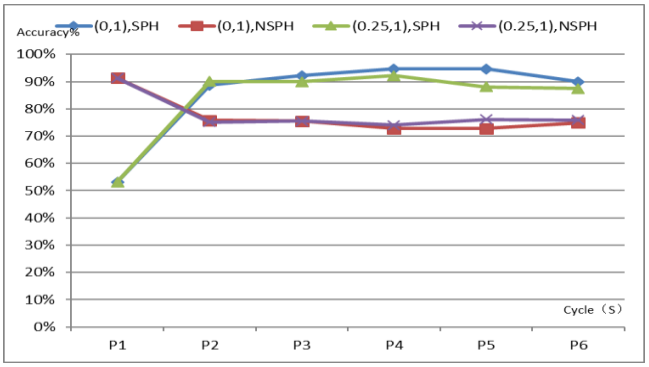

Fig. 2. Comparison of response time and throughput for component services.

V. SUMMARY

In this paper, an adaptive learning algorithm is used for the detection of spam host, this work is based on a large number of nested successful and unsuccessful forwarding messages in the SMTP session, as well as the embedded mail server information. The experimental results show that the adaptive learning algorithm can adjust the detector in a short period, and the detection success rate can be greatly improved. However, it is also found that some hosts may send spam through a simple mail transfer protocol based on the SSL security protocol or a pure web mail service, so finding a

robust and thorough solution is the next research direction.

ACKNOWLEDGMENT

The Paper is Supported by the fund: Special subject of China Association of Higher Education - Large data integration platform for the campus information intelligence user operation and maintenance services(2016XXYB02).

REFERENCES

[1] W. Y. Liu and T. Wang, "Online active multi-field learning foe efficient email spam filtering [J]," *Knowledge and Information Systems*, 2012, vol. 33, no. 1, pp. 117-136.
[2] J. R. Bertini *et al.*, "An incremental learning algorithm based on the K-associated graph for non-stationary data classification [J]," *Information Sciences*, 2013, vol. 246, pp. 52-68.
[3] J. Costa *et al.*, "Customized crowds and active learning to improve classification [J]," *Expert System with Application*, 2013, vol. 40, no. 18, pp. 7212-7219.
[4] Y. T. LI *et al.*, "Application of stacked denoising autoencoder in spamming filtering [J]," *Journal of Computer Applications*, 2015, vol. 35, 11, pp. 3256-3260.
[5] C. E. Shen *et al.*, "Spam filtering based on modified stack auto-encoder [J]," *Journal of Computer Applications*, 2016, vol. 36, no. 1, pp. 159-162.

Bin Chen was born in 1978. He is Ph.D. and engineer. His research interests include distributed computing and cloud computing.

Yizhou Dong was born in 1978. His research interests include internet of things application technology.

Mingrong Mao was born in 1958. His research interests include network application technology.