Rejecting Spam during SMTP Sessions

Muhammad N. Marsono† M. Watheq El-Kharashi‡ Fayez Gebali†
†Department of Electrical and Computer Engineering, University of Victoria, Victoria BC, Canada
‡Mentor Graphics Egypt, Cairo 11341, Egypt
E-mail: {mmarsono, watheq, fayez}@ece.uvic.ca

Abstract— **This paper analyzes a spam rejection scheme at Simple Mail Transfer Protocol (SMTP) sessions. This scheme utilizes a layer-3 e-mail pre-classification technique to estimate e-mail classes before an SMTP session ends. We study the spam rejection scheme using discrete-time Markov chain analysis and analyze the performance of the proposed scheme under different e-mail traffic loads and service capacities. The proposed scheme reduces the e-mail volume to be queued and processed by e-mail servers. This reduces non-spam e-mail queuing delay and loss, and protects e-mail servers from being overloaded by spam traffic.**

I. Introduction

Current spam control systems are post-acceptance systems [1]. E-mails are first received and buffered in a common queue before spam detection is performed. An e-mail class is only known after the e-mail is classified, i.e., after the Simple Mail Transfer Protocol (SMTP) [2] session ends. During heavy spam traffic, the non-spam e-mail delivery could be delayed and lost. Spam is best stopped before it is being received by the receiving e-mail server (also known as mail transfer agent, MTA) [3]. Spam detection during SMTP sessions is impossible without passing e-mail class hints (within the e-mail) or without a fast e-mail class estimation.

A fast and accurate e-mail class estimation on MTAs is possible by pre-classifying e-mails at layer 3 (the packet level) [4]. This paper analyzes a spam rejection scheme during SMTP sessions to reduce the number of e-mails received for delivery by MTAs and hence, non-spam queuing delay and loss probability. We model and estimate the performance of our proposed scheme at the receiving MTA using discrete-time Markov chain analysis. Our results show that the non-spam queuing delay and loss probability can be reduced due to the reduction in the number of e-mails to be processed by an MTA.

This paper is structured as follows. We discuss related works in Section II. Section III describes the spam rejection scheme. We model the proposed scheme in Section IV and analyze its performance in Section V. We conclude and state directions for future works in Section VI.

II. Related Works

Techniques to prioritize e-mail servicing on MTAs have been proposed in [1], [5]. Prioritizing e-mail servicing gives better non-spam delay and loss probability even under heavy e-mail loading and high spam prior [5]. Such techniques deal with e-mails after they are received for queuing. Our proposed scheme deals with e-mails before they are received for queuing.

A similar e-mail proxy technique that throttles attempted spam connections has been proposed in [6] using a proxy server due to the need for layer-7 spam detection. The authors' recent work showed that spam can be pre-classified at layer 3 anywhere in the network without the need to reassemble email messages [4]. By pre-classifying and tagging e-mail packets at intermediate nodes, a fast e-mail class estimation can be performed by the receiving MTAs. The layer-3 e-mail classification detects spam with 2% false positive (f_p) and 27% false negative (f_n) [4].

Spam control on outbound e-mail traffic can effectively control spam [7], especially when illegal zombie-relayed spam probability is high [8]. A zombie detection technique has been proposed in [9] by heuristically analyzing spam transfer and rejection behaviors from MTA logs. In our proposed spam rejection scheme, the failure in sending an e-mail, including failed spam deliveries to valid e-mail addresses are also negatively acknowledged and logged by sending MTAs. This provides easier log analysis compared to [9] since users with high e-mail rejection statistics are most likely relaying spam and not false positive senders.

III. Proposed Spam Rejection Scheme during SMTP Sessions

Fig. 1 shows an example of an SMTP session between two MTAs. Lines with `S` are those sent by the sender MTA, whereas lines with `R` are those sent by the receiving MTA. On line `05`, the envelope address `MAIL FROM` used to forward the e-mail does not have to be the same as the address `From` on line `11`, which specifies the author's e-mail address. The fields `To` and carbon copy (`Cc`) specify the e-mail recipients. The `Date` field specifies the date and time of the e-mail. As specified in RFC2822 [10], all header fields as well as e-mail body are free text input, which need not to be valid and can be easily forged.

Layer-3 pre-classification allows e-mail class estimation before an SMTP session ends, i.e., before an e-mail is accepted for queuing (line `21` in Fig. 1). The receiving MTA can issue a temporary failure notice (tempfail) [2] to deny e-mail receipt before the session ends. With this scheme, when a server's resources are low or the traffic loading is higher than the service capacity, a server could reject spam e-mails and deny an e-mail transfer at its SMPT session.

Fig. 2 illustrates the proposed spam rejection scheme during SMTP sessions. Current statistics show that more than two-thirds of the e-mail traffic over the Internet are spam e-mails [8]. For inbound spam control, spam transfers can be

Authorized licensed use limited to: UNIVERSITY TEKNOLOGI MALAYSIA. Downloaded on December 30, 2009 at 20:31 from IEEE Xplore. Restrictions apply.

```
01 S  telnet smtp.mail.net 25
      Trying <IP address>... Connected to smtp.mail.net
      (<IP address>). Escape character is '^]'.
02 R  220 smtp.example.net ESMTP Sendmail 8.12.11;
      Wed, 27 Dec 2006 12:00:00 +0100
03 S  EHLO smtp.mail.org
04 R  250-smtp.mail.net Hello smtp.mail.org <IP address>,
      pleased to meet you
05 S  MAIL FROM: <alice@mail.org>
06 R  250 2.1.0 <alice@mail.org>... Sender ok
07 S  RCPT TO: <bob@mail.net>
08 R  250 2.1.5 <bob@mail.net>... Recipient ok
09 S  DATA
10 R  354 Enter mail, end with "." on a line by itself
11 S  From: Alice <alice@mail.org>
12 S  To: Bob <bob@mail.net>
13 S  Cc: Charles <charles@mail.com>
14 S  Date: Wed, 27 Dec 2006 12:00:00 +0100 (CEST)
15 S  Subject: An E-mail Example
16 S
17 S  Hello,
18 S
19 S  This is an e-mail example, complete with a header
      and a body.
20 S  .
21 R  250 2.0.0 <queue ID> Message accepted for delivery
22 S  QUIT
23 R  221 2.0.0 smtp.mail.net closing connection
```

Fig. 1. E-mail transfer during an SMTP session.

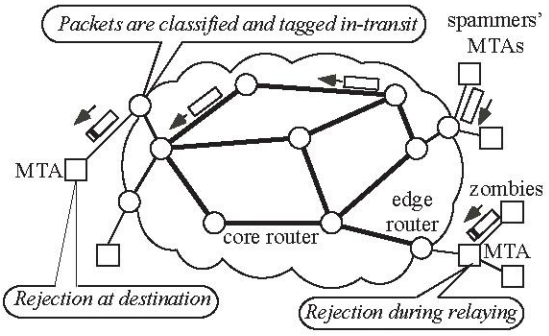

Fig. 2. Proposed spam rejection during SMTP sessions. Layer-3 e-mail pre-classification enables spam rejection of inbound spam and outbound spam during relaying.

denied without the need for queuing. This reduces the amount of e-mails to be processed by an MTA.

More than 45% of spam are relayed by zombie systems [8]. Spam rejection during SMTP sessions enables outbound spam control during relaying through legitimate MTAs. Similar to spam rejection at receiving MTAs, relaying MTAs can reject spam transfers at their SMTP sessions. Since rejection is at the SMTP session (layer 7), the delivery failure notice is issued to the sender MTA and can be used to detect zombie systems [9].

IV. Modeling the Proposed Spam Rejection Scheme

Fig. 3 shows the model of the proposed spam rejection scheme. E-mail packets are first reassembled (by module R) to form complete e-mails. During reassembly, e-mail classes can be estimated without significant delays when e-mail packets have been pre-classified and tagged with packet scores [4]. We define p_a as the probability that an e-mail is accepted during an SMTP session and queued in queue W. We also define p_d as the probability that an e-mail is dropped during an SMTP session. Then, e-mails are queued before being processed by a layer-7 spam detector C with a service probability c. Then, C decides whether to forward an e-mail to the recipient's mailbox or to a junk e-mail folder.

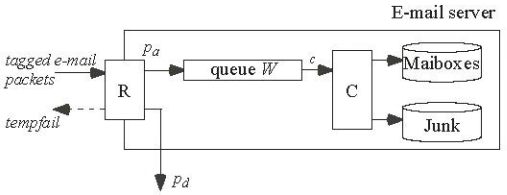

Fig. 3. The model of the proposed spam rejection during SMTP sessions. Suspected spam e-mails are dropped to reduce the amount of e-mails to be processed by an MTA.

The e-mail arrival can be measured by the e-mail inter-arrival time, which follows the exponential distribution [11]. The delay to detect spam can be measured by its service time, which is not sensitive to e-mail size and could be modeled using exponential distribution [1]. Define $\check{t}_a$ as the minimum e-mail inter-arrival time and $\check{t}_c$ as the minimum service time. Choosing a time step $\tau = min(\check{t}_a, \check{t}_c)$ ensures that an M/M/1/B Markov chain model [12] can be used to model the queue. The e-mail arrival probability can be defined as $a = \tau/t_a$, where t_a is the average e-mail inter-arrival time. Similarly, the service probability can be defined as $c = \tau/t_c$, where t_c is the average e-mail service time.

Due to the retransmission policy, a compliant MTA will attempt retransmission. We assume that spammers' own MTAs (not zombie systems) do not attempt retransmissions under the assumption that the recipients' addresses are invalid [1]. We also assume that senders' histories are maintained by the receiving MTA to accept e-mails after k_{max} retransmission attempts. Given p_s as the spam prior and p_z as the probability that spam is sent by a zombie, p_a and p_d are defined as

$$p_a = a(1-p_s) + ap_s(f_n + p_z t_n) \quad (1)$$

$$p_d = a(1-p_s) f_p (k_{max} - 1) + ap_s t_n (1 + p_z(k_{max} - 1)) \quad (2)$$

where $t_n = 1 - f_n$ is the true negative. Note that retransmission increases p_a by only one attempt since attempts $1 \leq k < k_{max}$ are rejected.

An M/M/1/B queue W of size B with the arrival probability p_a and service probability c can be analyzed using Markov chain analysis [12]. Assuming that an e-mail cannot arrive and be served in the same time step, the queue can be described by the state transition matrix

$$\mathbf{P} = \begin{bmatrix} 1-p_a & bc & \cdots & 0 & 0 \\ a & f & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & f & bc \\ 0 & 0 & \cdots & p_a d & 1-bc \end{bmatrix} \quad (3)$$

where $b = 1 - p_a$, $d = 1 - c$, and $f = p_a c + bd$. The equilibrium distribution vector $\mathbf{w}$ [12] can be expressed as

$$\mathbf{w} = \begin{bmatrix} w_0 & w_1 & \cdots & w_{B-1} & w_B \end{bmatrix}^t \quad (4)$$

where w_i is the probability that queue W contains i e-mails. At steady-state, solving $\mathbf{Pw} = \mathbf{w}$ and $\sum_{i=0}^{B} w_i = 1$ [12] gives

$$w_i = \frac{(1-\rho d)\rho^i d^{max(0,i-1)}}{1 + \rho(c - \rho^B d^B)} \quad \text{for } 0 \leq i \leq B. \quad (5)$$

where $\rho = p_a/(bc)$.

Authorized licensed use limited to: UNIVERSITY TEKNOLOGI MALAYSIA. Downloaded on December 30, 2009 at 20:31 from IEEE Xplore. Restrictions apply.

We are interested in two performance metrics, the non-spam queuing delay and loss probability. The average queue throughput, T, is defined as the probability that an e-mail be served [12] and is defined as

$$T = c(1 - w_0) \quad (6)$$

From [12], the average queue occupancy Q is given by

$$Q = \sum_{i=0}^{B} i w_i \quad (7)$$

From Little's result [12], the average queuing delay D_s is given by

$$D_s = \frac{Q}{T} = \frac{\sum_{i=0}^{B} i w_i}{c(1 - s_0)} \quad (8)$$

A non-spam e-mail is lost when the queue is full, or when a non-spam e-mail arrives and the queue is not served in a single time step (i.e., $t_c \geq \tau$). For the spam rejection scheme, the non-spam loss probability can be estimated as

$$L_s = \frac{a(1 - p_s)}{p_a} w_B p_a d \quad (9)$$

We analyzed typical single-queue scheme at receiving MTAs in our recent work on prioritized e-mail servicing [5]. The single-queue scheme does not support spam rejection during SMTP sessions. The queue performance metrics can be obtained using M/M/1/B queue model with input probability a and service probability c. From [5], the non-spam queuing delay of the current scheme, D is defined as

$$D = \frac{\sum_{i=0}^{B} i \; s_i}{c(1 - s_0)} \quad (10)$$

where s_i is the probability that the common queue contains i e-mails. The non-spam loss probability of the current scheme, L is defined as

$$L = s_B a d (1 - p_s) \quad (11)$$

V. Performance Analysis

This section analyzes the performance of our proposed spam rejection scheme. For all figures in this section, horizontal axes represent the arrival to service ratio $0 \leq a/c \leq 2$, where $a/c > 1$ and $a/c \leq 1$ illustrate an under-provisioned and an over-provisioned MTA, respectively. An under-provisioned MTA could not process all incoming e-mails. The vertical axes are for non-spam delay or loss probability for $B = 50$, $\tau = 0.1s$, and $k_{max} = 2$. Dashed lines represent the current (without SMTP rejection) and solid lines represent the proposed scheme.

A. Effect of p_s

Fig. 4 shows the performance of the proposed spam rejection scheme when $0.3 \leq p_s \leq 0.7$, $f_p = 0.02$, $f_n = 0.27$, and $p_z = 0.45$. Fig. 4(a) shows that the queuing delays decrease with increasing p_s, where $D_s < D$ for all a/c values. The non-spam loss probabilities show similar trend to the non-spam delay, as shown in Fig. 4(b). Both L_s and L decrease as p_s increases with $L_s < L$ for all a/c values. Since p_s directly affects p_a, we can conclude that higher p_s results in higher reduction in spam to be processed, and hence, lower non-spam queuing delay and loss probability.

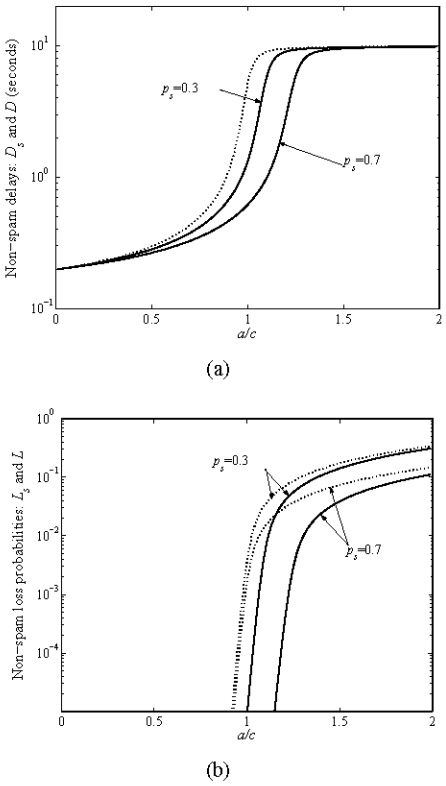

Fig. 4. Effects of p_s on the performance of rejecting spam during SMTP sessions when $p_s \in \{0.3, 0.7\}$, $0 < a/c < 2$, $f_p = 0.02$, $f_n = 0.27$, $p_z = 0.45$, $k_{max} = 2$, and $\tau = 0.1s$. (a) Non-spam queuing delays. b) Non-spam loss probabilities.

B. Effect of f_p

According to Equation (2), the input to the queue in our proposed spam rejection scheme, p_a, is not influenced by the changes in f_p and hence, D_s and L_s.

C. Effect of f_n

Fig. 5 shows the effect of f_n on the non-spam queuing delays and loss probabilities when $p_s = 0.5$, $f_p = 0.02$, $0 \leq f_n \leq 0.5$, and $p_z = 0.45$. Fig. 5(a) shows that the queuing delays increase as f_n increases with $D_s < D$ for all a/c values. Similar trend is observed for the non-spam loss probabilities, where increases in f_n increase L_s and L ($L_s < L$ for all a/c values). False negative, f_n affects the input probability to the queues, p_a. Increases in f_n increase the input probability to the queue and result in increases in D_s and L_s.

D. Effect of p_z

One of the main issues of spam rejection during SMTP sessions is zombie-relayed spam e-mails. Fig. 6 shows the effect of p_z on D_s and L_s when $p_s = 0.5$, $f_p = 0.02$, $f_n = 0.5$, and $0 \leq p_z \leq 0.9$. Fig. 6(a) shows that D_s and D increase as p_z increases, where $D_s < D$ for all a/c values. Similarly, Fig. 6(b) shows L_s and L ($L_s < L$ for all a/c values). Since p_z affects p_a, increases in p_z result in increases in D_s and L_s. From our analysis, we observed that the value of $p_z \leq 90\%$ gives better performance than the current scheme.

Authorized licensed use limited to: UNIVERSITY TEKNOLOGI MALAYSIA. Downloaded on December 30, 2009 at 20:31 from IEEE Xplore. Restrictions apply.

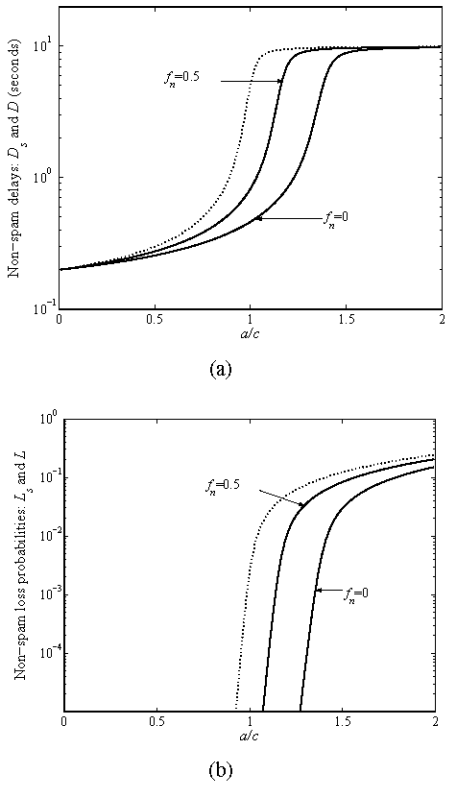

Fig. 5. Effects of f_n on the performance of rejecting spam during SMTP sessions when $p_s = 0.3$, $0 < a/c < 2$, $f_p = 0.02$, $f_n = \{0, 0.5\}$, $p_z = 0.45$, $k_{max} = 2$, and $\tau = 0.1s$. (a) Non-spam queuing delays. b) Non-spam loss probabilities.

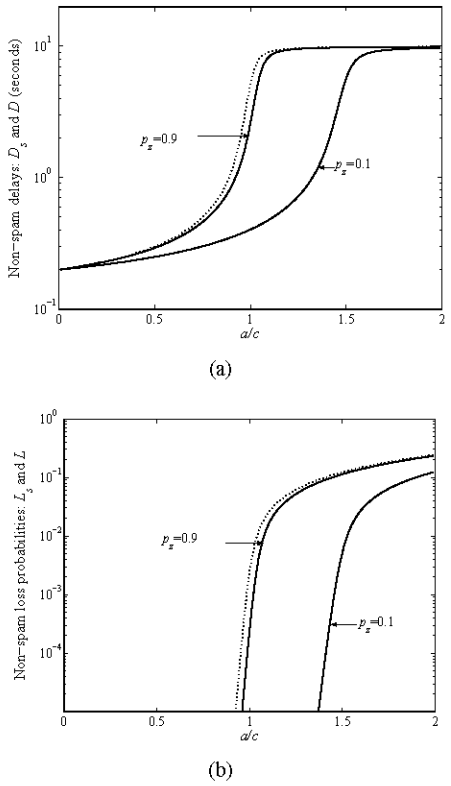

Fig. 6. Effects of p_z on the performance of rejecting spam during SMTP sessions when $p_s = 0.5$, $0 < a/c < 2$, $f_p = 0.02$, $f_n = 0.5$, $p_z \in \{0, 0.9\}$, $k_{max} = 2$, and $\tau = 0.1s$. (a) Non-spam queuing delays. b) Non-spam loss probabilities.

VI. Conclusion and Future Work

We proposed and evaluated a spam rejection scheme during SMTP sessions. We analyzed the performance and cost of the proposed scheme. We found that the proposed spam rejection scheme exhibits better non-spam delay and non-spam loss probability than the single-queue scheme without SMTP rejection. The proposed scheme protects MTAs from being overloaded by huge incoming spam traffic.

This work can be further extended to proposing a scheme to detect and reduce the zombie problem and illegal spam relaying. It can also be extended to spam throttling beyond MTAs by utilizing the layer-3 e-mail classification technique and developing a hardware architecture for e-mail class estimation.

Acknowledgments

The first author is funded by Malaysian Government scholarship JPA-UTM JPA(L)A-3238549. He is with the Faculty of Electrical Engineering, Universiti Teknologi Malaysia.

References

[1] R. D. Twining, M. M. Williamson, M. Mowbray, and M. Rahmouni, "Email prioritization: Reducing delays on legitimate mail caused by junk mail," HP Digital Media Systems Laboratory, Bristol, UK, Technical Report HPL-2004-5(R.1), May 2004. [Online]. Available: http://www.hpl.hp.com/techreports/2004/HPL-2004-5R1.pdf

[2] J. Klensin. (2001, April) RFC2821: Simple mail transfer protocol. [Online]. Available: http://www.ietf.org/rfc/rfc2821.txt

[3] S. Hird, "Technical solutions for controlling spam," in *Proceedings of the Australian UNIX and Open Systems User Group (AUUG)*, Melbourne, Australia, September 2002. [Online]. Available: http://security.dstc.edu.au/papers/technical_spam.pdf

[4] M. N. Marsono, M. W. El-Kharashi, F. Gebali, and S. Ganti, "A distributed e-mail classification for spam control," in *Proceedings of the 2006 Canadian Conference on Electrical and Computer Engineering (CCECE 2006)*, Ottawa, ON, Canada, May 2006, pp. 438–441.

[5] M. N. Marsono, M. W. El-Kharashi, and F. Gebali, "Performance analysis of server-side spam control strategies based on layer-3 classification," in *Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2007)*, Vancouver, BC, Canada, April 2007, pp. 349–352.

[6] M. Tran and G. Armitage, "Evaluating the use of spam-triggered TCP/IP rate control to protect SMTP servers," in *Proceedings of the Australian Telecommunications Networks & Applications Conference (ATNAC)*, Sydney, Australia, December 2004, pp. 329–335.

[7] J. Goodman and R. Rounthwaite, "Stopping outgoing spam," in *Proceedings of the ACM Conference on Electronic Commerce (EC'04)*, New York, NY, USA, May 2004, pp. 30–39.

[8] (2007, May) The real threat of spam. [Online]. Available: http://whitepapers.silicon.com/0,39024759,60131105p-39000647q,00.htm

[9] R. Clayton, "Stopping spam by extrusion detection," in *Proceedings of the First Conference on Email and Anti-Spam (CEAS)*, Mountain View, CA, USA, July 2004. [Online]. Available: http://www.ceas.cc/papers-2004/172.pdf

[10] P. Resnick. (2001, April) RFC2822: Internet message format. [Online]. Available: http://www.ietf.org/rfc/rfc2822.txt

[11] L. H. Gomes, C. Cazita, J. M. Almeida, V. Almeida, and J. Wagner Meira, "Characterizing a spam traffic," in *Proceedings of the Fourth ACM SIGCOMM Conference on Internet Measurement (IMC)*, Taormina, Italy, October 2004, pp. 356–369.

[12] F. Gebali, *Computer Communications Networks: Analysis and Design*, 3rd ed. Victoria, BC, CA: North Star Digital Design, 2004.

Authorized licensed use limited to: UNIVERSITY TEKNOLOGI MALAYSIA. Downloaded on December 30, 2009 at 20:31 from IEEE Xplore. Restrictions apply.