Robust Estimation of Message Importance using Inferred Inter-Recipient Trust for Supporting Email Triage

Sho Tsugawa Kazuya Takahashi Hiroyuki Ohsaki Makoto Imase
Graduate School of Information Science and Technology
Osaka University, Suita, Osaka 565-0871, Japan
email:{s-tugawa,k-takahashi,oosaki,imase}@ist.osaka-u.ac.jp

***Abstract*—In recent years, the number of emails received by an individual has been increasing, and the time required for *email triage* (i.e., the process of going through unhandled emails and deciding what to do with them) has therefore been increasing. Golbeck *et al.* proposed TrustMail, which is a prototype email client that prioritizes emails in user's mailbox utilizing a trust network (i.e., a social network representing trust relationships among users). In this paper, we extend the notion of TrustMail to allow robust message-based prioritization using inter-recipient trusts, which are (inferred) trust scores from the recipient to other recipients. We propose a method called *EMIRT (Estimating Message Importance from inter-Recipient Trust)* for enabling robust message prioritization. We also evaluate the effectiveness of our proposed EMIRT for estimating importance of emails through experiments utilizing a large email corpus called Enron Email Dataset. Consequently, we show that EMIRT realizes robust email prioritization.**

***Keywords*-email triage; trust; social network; robust prioritization;**

I. Introduction

In recent years, the number of emails received by an individual has been increasing, and the time required for *email triage* (i.e., the process of going through unhandled emails and deciding what to do with them) has therefore been increasing. For instance, it is reported that 16% of employees in a corporation have spent one hour or more per day just for email triage [1]. It is also reported that 46% of employees, who receive 100 or more emails per day (i.e., heavy email users), have spent one hour or more per day just for email triage [1].

On the contrary, trust information in a social network has been becoming popular these days. For instance, in a social networking service called Orkut [2], participants are allowed to give trust scores to their acquaintances in four levels, which are visible to other users. Also, in other services such as Moleskiing [3] and FilmTrust [4], participants are allowed to give trust scores to their acquaintances.

In [5], Golbeck *et al.* proposed TrustMail, which is a prototype email client that prioritizes emails in user's mailbox utilizing a trust network (i.e., a social network representing trust relationships among users). TrustMail is the pioneering work in email triage utilizing a trust network. TrustMail assumes that the trust network is accessible by the TrustMail; i.e., trust scores from a person to his/her acquaintances are registered, and those trust scores are available. When a user receives an email from a stranger, TrustMail prioritizes the email by inferring the trust score from the recipient to the stranger (i.e., sender trust) utilizing the *transitivity* property (i.e., if A trusts B and B trusts C, A should trust C) in a trust network [5].

TrustMail has several clear advantages. TrustMail can prioritize emails, whose senders are unknown by the recipient. TrustMail can prioritize those emails by inferring trust scores from the recipient to unknown senders by traversing a trust network [5]. Also, TrustMail requires little configuration burden on users; i.e., users are just required to update trust scores of their acquaintances, which are not likely to change frequently.

We believe an approach of TrustMail is novel yet there remain several open issues. For instance, TrustMail adopts a sender-based prioritization. If the sender trust cannot be inferred (i.e., the recipient and the sender are not reachable in the trust network), TrustMail cannot prioritize the email. Moreover, inference error in the sender trust directly affects the accuracy of the email prioritization. Namely, TrustMail is robust against neither failure nor error in the sender trust inference.

In this paper, we therefore extend the notion of TrustMail to allow robust message-based prioritization using inter-recipient trusts, which are (inferred) trust scores from the recipient to other recipients. We propose a method called *EMIRT (Estimating Message Importance from inter-Recipient Trust)* for enabling robust message prioritization. EMIRT can realize robust email prioritization not only using the sender trust but also using the inter-recipient trusts. We also evaluate the effectiveness of our proposed EMIRT for estimating importance of emails through experiments utilizing a large email corpus called Enron Email Dataset [6]. Consequently, we show that EMIRT realizes robust email prioritization.

The organization of this paper is as follows. Section II introduces TrustMail and its algorithm for inferring the sender trust (i.e., the trust score from the recipient to the stranger). Our EMIRT, which realizes robust message-based prioritization utilizing inter-recipients trusts, are presented in Section III. Section IV is devoted for performance evaluation of our proposed EMIRT through experiments utilizing a large email corpus. Finally, Section V concludes this paper and discusses future works.

II. TrustMail and Trust Inferring Algorithm

In this section, we introduce TrustMail [5] and its algorithm for inferring the sender trust (i.e., the trust score from the recipient to the stranger).

In [5], Golbeck *et al.* proposed TrustMail, which is a prototype email client that prioritizes emails in user's mailbox utilizing a trust network (i.e., a social network representing trust relationships among users). In TrustMail, a trust network is represented as a weighted directed graph $G = (V, E)$. A link (i, j) with weight $w_{i,j}$ represents a trust score from user i to user j. A weight $w_{i,j}$ ranges between 0 and 1, and 0 means user i does not trust user j. TrustMail prioritizes emails even from strangers by inferring the sender trust (i.e., trust scores of unknown senders) [5].

In what follows, we briefly explain the algorithm for inferring a trust score from node s to node d using a trust network. Figure 1 illustrates an example of trust inference using a trust network. Refer to [5] for the details of the trust inferring algorithm.

Basically, the trust score from node s to node d, $T(s, d)$, is inferred by recursively traversing the trust network using a depth-first search (DFS) algorithm.

(1) Initialization
Make the originating node s be the current node i; $i \leftarrow s$. The set of visited nodes S is initialized to empty; $S \leftarrow \{\}$.

(2) Check acquaintances
If node i has a trust score to node d, return the trust score $w_{i,d}$. Namely, return $w_{i,d}$ as $T(i, d)$ if $(i, d) \in E$. Otherwise, proceed to the next step.

(3) Obtain trust scores from all unvisited neighbors
Ask all unvisited neighbors of node i to return their trust scores for node d. Namely, for all nodes j's with $(i, j) \in E$ and $j \notin S$, obtain $T(j, d)$'s by recursively performing the algorithm from the step (2) with $i \leftarrow j$. Add j's to the set of visited nodes S; $S \leftarrow S \cup \{j\}$.

(4) Average trust scores
Calculate the weighted mean of trust scores obtained from all unvisited neighbors, and terminate the algorithm. Namely,

$$T(i, d) = \sum_j w_{i,j} \, T(j, d). \qquad (1)$$

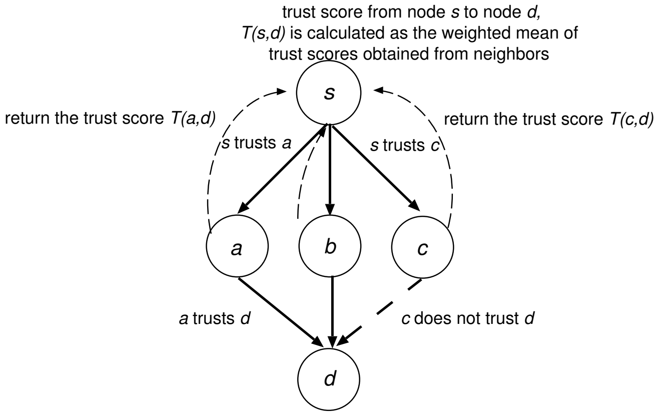
trust score from node s to node d,
T(s,d) is calculated as the weighted mean of
trust scores obtained from neighbors
s
return the trust score T(a,d)
return the trust score T(c,d)
s trusts a
s trusts c
a
b
c
a trusts d
c does not trust d
d

Figure 1: An example of trust inference using a trust network

Thus, if node s gives a trust score to node d (i.e., $(s, d) \in E$), $T(s, d)$ is the trust score $w_{s,d}$. If node d is not reachable from node s (i.e., there exists no path from node s to node d), $T(s, d) = 0$.

In [5], two algorithms, *rounding algorithm* and *non-rounding algorithm*, are discussed since the authors only focus on binary trust (i.e., trust or don't trust). In the rounding algorithm, $T(i, d)$ obtained in the step (4) is rounded to the nearest integer (i.e., 0 or 1). In the non-rounding algorithm, $T(s, d)$ is rounded to the nearest integer, but other $T(i, d)$'s are not rounded.

In this paper, we use *never-rounding algorithm* for inferring a continuous trust score from node s to node d. $T(i, d)$ is used as-is, i.e., $T(i, d)$ in the step (4) is never rounded to the nearest integer.

Table I
DEFINITION OF SYMBOLS

symbol	definition
m	email
s	sender of email m
r	recipient of email m
$R(m)$	set of recipients of email m
$T(i, j)$	trust score from node i to node j
$P(m, r)$	estimated importance of email m for recipient r

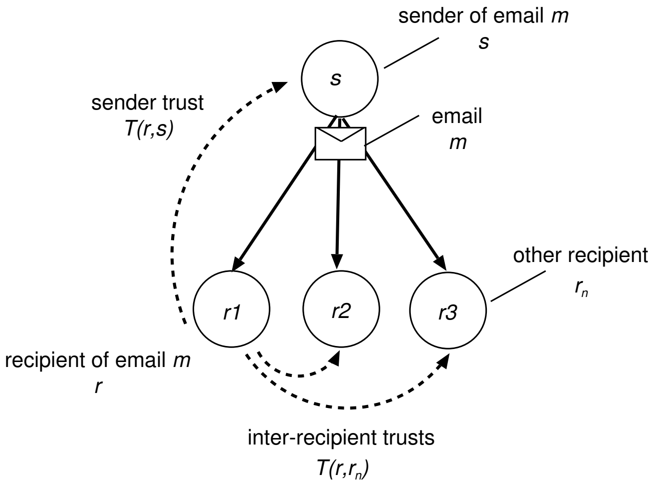

Figure 2: The meaning of each symbol

III. EMIRT (ESTIMATING MESSAGE IMPORTANCE FROM INTER-RECIPIENT TRUST)

In this section, we propose a method called EMIRT (Estimating Message Importance from inter-Recipient Trust) for enabling robust message prioritization. The definition of symbols used in this paper is summarized in Tab. I. Meaning of those symbols is illustrated in Fig. 2.

EMIRT prioritizes an email based on the idea that the higher the sender trust is and *the higher the inter-recipient trusts are*, the more important the email should be. Email has been widely used for multicast-style communications. Hence, in many cases, we can utilize not only the sender trust but also inter-recipient trusts (i.e., trust from the recipient to other recipients). By utilizing multiple trust scores, it is expected that EMIRT can realize robust email prioritization.

Similarly to TrustMail, our EMIRT assumes that the trust network is accessible. As discussed in [5], it is expected that a trust network will be accessible in the future.

EMIRT prioritizes an email by inferring the trust scores from recipient r to the other recipients r_n, $T(r, r_n)$, and to the sender s, $T(r, s)$, from the trust network using the trust inferring algorithm introduced in Section II. Other recipients r_n are known from the header (e.g., `To` and `Cc` fields) of the email. Specifically, the importance of email m for recipient r is given by

$$P(m, r) = \sum \xi_{r,s} T(r, s) + \sum \xi_{r,r_n} T(r, r_n), \qquad (2)$$

where $\xi_{r,s}$ and ξ_{r,r_n} are parameters determining the balance between the sender trust score $T(r, s)$ and inter-recipient trust scores $T(r, r_n)$. Note that the trust score from recipient r to himself/herself is defined as $T(r, r) = 1$.

Desired settings of those weights, $\xi_{r,s}$ and ξ_{r,r_n}, should be dependent on several factors such as the objective of email communication and the style of email usage. In this paper, for simplicity, we use the following values.

$$\xi_{r,s} \quad = \quad \xi_{r,r_n} = \frac{1}{1 + |R(m)|} \qquad (3)$$

In the above equation, $1 + |R(m)|$ denotes the number of people involved in the email communications (i.e., sender and recipients). Thus, the sender trust score and each of inter-recipient trust scores are equally weighted.

IV. EXPERIMENTS

A. Methodology

In this section, we evaluate the effectiveness of our proposed EMIRT for estimating importance of emails through experiments utilizing a large email corpus called *Enron Email Dataset* [6].

Enron Email Dataset contains 517,431 emails with headers and body texts of 150 users in Enron Corporation. To the best of our knowledge, Enron Email Dataset is the only real corporate email dataset available to public, which has been used for several researches [7]. Because of its size and availability, Enron Email Dataset should be useful for evaluating the effectiveness of our proposed EMIRT.

For evaluating the effectiveness of our proposed EMIRT, we investigate the correlation between the estimated importance of emails and the time-to-reply of emails. It is expected that important emails are likely to be replied quickly compared to non-important emails.

First, the time-to-reply for each email in Enron Email Dataset is obtained. Since the `Reply-To` field is missing in the header of emails in Enron Email Dataset, we analyze the correspondence between the original email and the replying email. Specifically, if a user receives an email and he/she returns an email to the sender with the same subject with a prefix `Re:`, those two emails are considered as the original email and the replying email, respectively. The time-to-reply

Table II
AVERAGE AND STANDARD DEVIATION OF INFERRED SENDER TRUST AND ESTIMATED IMPORTANCE FOR EACH CATEGORY

	inferred sender trust		estimated importance	
	average	standard deviation	average	standard deviation
1 day	0.83	0.37	0.88	0.21
3 days	0.74	0.44	0.81	0.26
1 week	0.72	0.44	0.79	0.25
not replied	0.54	0.49	0.71	0.29

for the original email is obtained as the elapsed time between receiving the original email and sending the replying email.

Second, the trust network (i.e., a social network representing trust relationships among users) among users in Enron Email Dataset is obtained. The trust network is required to infer the trust score among users. We assume the existence of positive correlation between the trust score and the frequency of email exchanges. Hence, the trust network is built from the frequency of email exchanges among users. Specifically, the trust network is created as a weighted directed graph $G = (V, E)$. A link is created from node i to node j if no less than five emails are sent from user i to user j. All weights of links are equally set to 1 for simplicity.

B. Results and Discussions

For investigating the correlation between the importance of emails estimated with EMIRT and the time-to-reply of emails, we classified emails into four categories based on their time-to-reply (i.e., one day, three days, one week, and not replied). We calculated the average and the standard deviation of importance $P(m, r)$'s estimated with EMIRT for each category. The average and the standard deviation are shown in Tab. II. For comparison purpose, the average and the standard deviation of inferred sender trusts for each category are also shown in Tab. II. Note that the inferred sender trust is equivalent to the metric used in TrustMail for prioritizing emails except that TrustMail uses either rounding or non-rounding algorithms whereas the never-rounding algorithm is used in our experiments. In this experiment, we randomly sampled 1,000 emails from emails in each category.

From the average of inferred sender trusts and estimated importance $P(m, r)$'s for each category, one can find that both estimated importance with EMIRT and inferred sender trusts succeed to appropriately prioritize emails. Wilcoxon test with p = 0.05 [8] indicates that there exist significant difference in these averages.

By comparing the standard deviations of inferred sender trusts and estimated importance $P(m, r)$'s for each category, one can find that the standard deviations of the inferred sender trust are significantly larger than those of estimated importance. Namely, EMIRT realizes robust email prioritization using inter-recipients trust.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a method called EMIRT (Estimating Message Importance from inter-Recipient Trust) enabling robust message prioritization. We have also evaluated the effectiveness of our proposed EMIRT for estimating importance of emails through experiments utilizing a large email corpus called Enron Email Dataset. Consequently, we have shown that EMIRT realizes robust email prioritization.

As future work, we are planning to extend our EMIRT to include other factors than trust for improving the accuracy of prioritization.

ACKNOWLEDGEMENTS

The authors would like to thank Prof. Masayuki Murata for his kind support and valuable discussions.

This research was partly supported by “Global COE (Centers of Excellence) Program” of the Ministry of Education, Culture, Sports, Science and Technology, Japan.

REFERENCES

[1] C. Neustaedter, A. B. Brush, and M. A. Smith, “Beyond “from” and “received”: Exploring the dynamics of email triage,” in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2005)*, pp. 1977–1980, Apr. 2005.

[2] “Orkut.” http://www.orkut.com/.

[3] P. Avesani, P. Massa, and R. Tiella, “A trust-enhanced recommender system application: Moleskiing,” in *Proceedings of the 2005 ACM Symposium on Applied Computing (SAC 2005)*, pp. 1589–1593, Mar. 2005.

[4] J. Golbeck and J. Hendler, “Filmtrust: Movie recommendations using trust in Web-based social networks,” in *Proceedings of the IEEE Consumer Communications and Networking Conference*, pp. 282–286, Jan. 2006.

[5] J. Golbeck and J. Hendler, “Inferring binary trust relationships in Web-based social networks,” *ACM Transactions on Internet Technology*, vol. 6, pp. 497–529, Nov. 2006.

[6] “Enron email dataset.” http://www.cs.cmu.edu/~enron/.

[7] J. Shetty and J. Adibi, “Discovering important nodes through graph entropy the case of Enron email database,” in *Proceedings of the 3rd international workshop on Link discovery*, pp. 74–81, Aug. 2005.

[8] F. Wilcoxon, “Individual comparisons by ranking methods,” *Biometrics*, vol. 1, pp. 80–83, Dec. 1945.