Legitimate E-mail Forwarding Server Detection Method by X-means Clustering Utilizing DMARC Reports

Kanako Konno
Department of Computer and Information Sciences,
Graduate School of Engineering,
Tokyo University of Agriculture and Technology
Tokyo, Japan
Email: k_konno@net.cs.tuat.ac.jp

Naoya Kitagawa
Division of Advanced Information Technology
and Computer Science,
Institute of Engineering,
Tokyo University of Agriculture and Technology
Tokyo, Japan
Email: nakit@cc.tuat.ac.jp

Shuji Sakuraba
Application Service Department,
Network Division,
Internet Initiative Japan Inc.
Tokyo, Japan
Email: saku@iij.ad.jp

Nariyoshi Yamai
Division of Advanced Information Technology
and Computer Science,
Institute of Engineering,
Tokyo University of Agriculture and Technology
Tokyo, Japan
Email: nyamai@cc.tuat.ac.jp

***Abstract*—There are several effective spoofed e-mail countermeasures, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC). However, these verification methods have an issue of erroneously determining many forwarded e-mails as malicious spoofing e-mails. When an e-mail is forwarded, the sender's IP address is changed to the forwarder's, thus the receiver cannot verify whether the e-mail is legitimate or not. On the other hand, DMARC has a function, which e-mail senders can receive DMARC aggregate reports that include information about e-mails, such as the authentication results of SPF and DKIM. In this paper, we propose a method to classify legitimate forwarding servers by X-means clustering analysis using a large number of summarized DMARC aggregate reports data. In addition, we apply our method to 5,366 e-mail sending servers that send 207,193,987 e-mails in total. As a result of the clustering, our method detects 451 servers as legitimate forwarders' server. As a result of verification of these servers by utilizing the IP blacklists and the spam filter results, we confirmed that 451 servers are legitimate e-mail sending server. On the other hand, 50.17% in median of the e-mails delivered from these 451 servers are erroneously failed in DMARC authentication. Thus, our method can significantly reduce DMARC verification's False Positives, and e-mail server administrators can detect many legitimate forwarded messages.**

***Keywords*–Spoofed e-mail; SPF; DKIM; DMARC; Clustering.**

I. Introduction

E-mail is one of the most convenient communication services all over the world. However, especially in business, e-mail has a serious problem that spoofed e-mails are increasing rapidly. According to the statistics report of FBI, the total financial damage is 12.5 billion US dollar from October 2013 to May 2018 [1]. Spoofing e-mails are abused by spammers to steal sensitive information or send malicious programs, such as computer virus.

Sender domain authentication has been proposed as an effective method to measure the spoofed e-mails. SPF [2] and DKIM [3] are widely used in the world. In SPF mechanism, the receivers check the sender's SPF record include IP addresses which the senders use to send e-mails, and confirm whether the e-mails senders are legitimate or not. However, SPF cannot verify forwarded messages correctly, because the sender's IP address is changed to the forwarder's IP address which is not included in the sender's SPF record when the e-mails are forwarded. In DKIM, the receivers verify the digital signatures generated from e-mails header and body and confirm whether the e-mail has not been rewritten by spammers. DKIM allows third parties to sign e-mails, thus DKIM has a problem that spoofed e-mails signed by a spammer's own malicious domain pass the verification incorrectly.

DMARC [4] is one of the most effective frameworks which has reporting and policy controlling mechanism in sender domain authentication. DMARC utilizes SPF and DKIM authentication mechanisms. In addition, DMARC has a concept called "alignment" which does not allowed third party's signature. Thus, DMARC is effective method to measure spoofed e-mail, however, DMARC cannot solve the issue that SPF cannot properly verify forwarded messages. For example, when an e-mail which is forwarded and signed by third party's domain, SPF verification is failed and DKIM verification is also failed with DMARC alignment.

DMARC has reporting function that allows a sender to receive "DMARC aggregate report" (hereinafter, this is called DMARC report). This report indicates information, such as e-mails header and the authentication results. In general, DMARC reports are utilized to confirm the effectiveness of sender domain authentications by the e-mail senders. On the other hand, we can observe the transmission behaviors for each e-mail sending servers by analyzing the information of DMARC reports. Moreover, we consider that forwarding servers have similarity in trends of e-mail transmission behaviors.

In this paper, we propose a method to detect legitimate forwarding servers by X-means clustering analysis utilizing massive DMARC reports data. Our approach divides the sender's IP addresses into some clusters. In addition, we identify the forwarder's cluster based on several already-known forwarders' IP addresses. We compare our clustering results and Spamhaus blocklist and results of Internet Service Provider (ISP)'s spam filter in order to evaluate our approach. As a result, our approach detects 451 legitimate forwarding servers that may verified as malicious servers by the conventional verification methods. Thus, e-mail administrators can detect many legitimate forwarding servers by utilizing our method when they know a few forwarding servers, such as ther own organization's servers beforehand.

This paper organized as follows. In Section II, we explain some anti-spam methods as related works. In Section III, we describe the design of our mechanism. Then we show the dataset which we utilize the experiment in Section IV. Section V shows results of our method applying and evaluate the validity of the servers classified as forwarding servers by our method. Finally, we present the concluding remarks in Section VI.

II. Related work

A large number of anti-spam methods have been proposed over the years. Contents filtering is an effective and widely used anti-spam method. For example, Bayesian Filter [5] [6] is a famous contents filtering method utilizing Bayes theorem. In addition, Natural Language Processing [7], support vector machines [8] [9], and machine learning [10] [11] are widely utilized. In actual operation, therefore contents filtering is high calculation cost, it is used after reducing the number of e-mails to be inspected by other anti-spam methods in advance.

SpamAssassin [12] [13] scores e-mails based on keyword, public database, and Bayesian Filter, etc., in order to detect spam e-mails. This method utilizes several anti-spam methods, such as Blacklist [14] [15] and sender domain authentication methods when the e-mails are received before Bayesian Filter.

Blacklist detects spammers utilizing a list including attackers' IP addresses and domains. Sender domain authentication methods can verify whether the e-mails are spoofed or not based on the information of e-mail senders.

SPF, DKIM, and DMARC are popular methods among sender domain authentication. We explain these three methods in the following subsections, II-A and II-B.

A. SPF & DKIM

SPF and DKIM are widely utilized methods as sender domain authentication.

SPF uses a SPF record to check whether IP address of sender's SMTP server is legitimate or not. SPF record indicates a list of server's IP addresses that the senders may use to send e-mails. The sender domain's administrator should publish an SPF record on their own authoritative DNS server beforehand. The receiver asks the SPF record of the sender's DNS server using sender's Envelope-From domain, then verifies whether the IP address of the sender's SMTP sever is included in the SPF record. However, SPF has a problem that SPF verification cannot authenticate forwarded messages properly, because the IP address of the original SMTP server changes to the IP address of the forwarding server, which is not included in the SPF record.

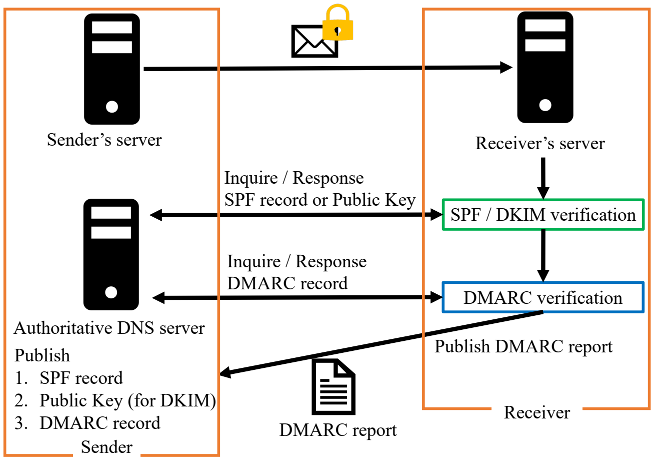

Figure 1. Flow of DMARC verification.

DKIM is an authentication method using digital signature (hereinafter, this is called "DKIM signature") generated from e-mail header and body. In order to use DKIM mechanism, the sender domain should prepare a pair of a private key and public key in advance and publish the public key on their authoritative DNS server. The sender domain generates a DKIM signature from the e-mail body and header using private key, and attaches it to "b=" tag of the e-mail header as the DKIM signature. Next, the receiver inquires the public key to the authoritative DNS server of sender's domain that is obtained in "d=" tag of the e-mail header. The receiver compares the hash value obtained from DKIM signature using the public key with the value of "bh=" tag. When these values are the same, the e-mail is passed the DKIM verification. With this mechanism, DKIM can verify forwarded messages correctly unlike SPF. Although DKIM allows third party domains to sign e-mails, it has an issue which the spoofed e-mails signed with spammers' own malicious domain will be passed the verification.

B. DMARC

DMARC is a reporting and policy controlling framework utilizing SPF and DKIM mechanism to authenticate e-mails.

Figure 1 shows the flow of DMARC verification. In order to use DMARC, the sender domain administrator must publish SPF record for SPF verification and public key for DKIM verification on the authoritative DNS server beforehand to utilize SPF and DKIM mechanism. Moreover, the sender domain needs to publish the DMARC record on their DNS server. For example, when the sender domain is "example.com", DMARC record is published as TXT record of "_dmarc.example.com" in the following rules.

```
v=DMARC1; p=reject; rua=mailto:rua@example.com
```

In policy controlling function, DMARC provides a mechanism for the sender domain's administrator to declare the policy how the receiver handles the e-mail, which fails sender domain authentication in the "p=" tag of the DMARC record. The value of "p=" tag has three variations, "none (do not anything even if authentication failure)", "quarantine (quarantine the authentication failure e-mail)", and "reject (reject the authentication failure e-mail)".

In reporting function, an e-mail receiver sends DMARC reports to e-mail address of sender domain's administrator shown in "rua=" tag of DMARC record.

DMARC report provides information, such as e-mail domains, authentication results, and effectiveness of DMARC policy. The examples of information included in DMARC reports are as follows.

- DMARC reporter's name
- Strictness of DMARC alignment
- Handling policy published by sender for failure e-mails (shown in "p=" tag of DMARC record)
- The IP address of the sender's server
- Disposition of e-mails based on DMARC policy
- DKIM authentication result when DMARC alignment is applied
- SPF authentication result when DMARC alignment is applied
- Header-From domain
- Envelope-From domain
- DKIM signature domain
- DKIM authentication result
- SPF authentication result

Thus, the sender domain's administrator can obtain the performance of DMARC authentication from DMARC reports, and they can take measures to prevent spoofed e-mails abusing their domain.

With the concept of "alignment", DMARC verification will be failed when domains for SPF and DKIM verification are different from the sender's Header-From domain. The sender's Header-From domain need not be the same as the Envelope-From domain or the DKIM signature domain. On the other hand, spammers can fraud the Header-From domain easily. As a countermeasure against this issue, by utilizing alignment, the receiver can check whether the Header-From domain is correct or not. The sender domain can choose from two strictness of alignment, "strict" and "relaxed", using DMARC record. When the sender domain's administrator uses "strict" mode, DMARC verification passes only when Header-From address and domain for SPF or DKIM verification match completely. On the other hand, when the alignment mode is "relaxed", DMARC verification will success if subdomains of Header-From address and subdomains of domain for SPF or DKIM verification match.

DMARC is one of the effective countermeasure to spoofed e-mail. However, DMARC cannot solve the issues that SPF cannot properly verify forwarded messages. As mentioned above, DMARC utilizes SPF and DKIM mechanism to authenticate e-mail. SPF cannot authenticate forwarded messages because the sender's IP address changes to forwarder's IP address when the e-mails are forwarded. Moreover, although DKIM allows third party's signature, which utilized widely over the world, the e-mails signed by third party's signer will be failed the DMARC verification due to alignment. Therefore, there are cases that legitimate forwarded messages will be failed the DMARC authentication, for example, when the e-mails utilize third party's signature or the e-mail's domains are not compatible with DKIM.

III. Design of our method

As described in subsection II-B, DMARC cannot solve the problem of SPF about forwarded messages. To overcome this issue, we propose a method adopting X-means clustering analysis to massive DMARC report data.

X-means clustering is K-means extended algorithm proposed by D.Pelleg and A. Moore [16]. K-means has been utilized as one of the most popular clustering methods. However, K-means has shortcoming which the number of clusters K has to be provided by users in advance. On the other hand, X-means can determine the number of clusters X by iterations of k-means and splitting decision based on Bayesian Information Criterion (BIC). Our method utilizes X-means clustering analysis in order to classify the sender's IP address.

Figure 2 shows the flow of our method. At first, in order to adapt X-means clustering analysis to DMARC reports, our approach summarizes the DMARC reports focus on the sender domain authentication results and the e-mail domains.

As the summarization of sender domain authentication results, we calculate the acceptance rate of SPF, DKIM, and DMARC for each sender's IP addresses. SPF, DKIM, and DMARC have several types of results as shown in Figure 2. Thus, our approach calculates not only the percentage of the authentications pass e-mails but also the percentage of other authentication results e-mails, such as "fail", "none", and so on.

In summarization the domain agreement rate part in in Figure 2, our approach calculates the percentage of e-mails which combinations of domains 1), 2), and 3) in Figure 2 are same or different for each combinaitons.

As described in subsection II-B, DMARC mechanism compares the combinations of Envelope-From domain and Header-From domain (combination 1) in Figure 2) for SPF alignment of DMARC. In addition, the combinations of Header-From domain and DKIM signature domain (combination 2) in Figure 2) are compared for DKIM alignment of DMARC. Although Envelope-From domain, Header-From domain, and DKIM signature domain are not necessarily the same because SPF and DKIM allows using third party domains to verify the e-mails, the domains combinations 1) and 2) have relations in DMARC authentication mechanism.

On the other hand, there is no need to compare the combinations of Envelope-From domain and DKIM signature domain (combination 3) in Figure 2) in SPF, DKIM, and DMARC verification processes. However, since the combinations 1) and 2) has relationships in sender domain authentications, we can considered that the combination 3) also has a relationship, such as rules of domain naming. Thus, we utilize domains combination 3) in order to improve accuracy of our method.

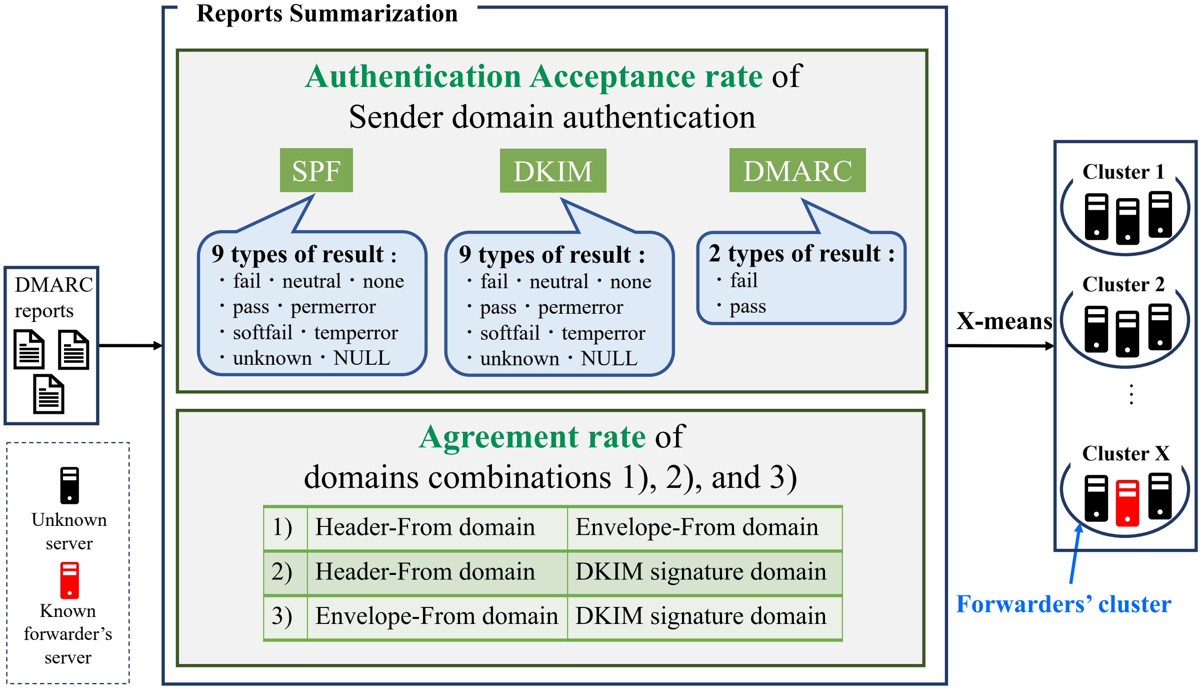

Figure 2. Design of our method.

Then, we classify the sender's IP addresses by X-means clustering analysis utilizing summarized DMARC reports information. As the result of X-means clustering analysis, the sender's IP addresses are divided into some clusters according to their e-mail transmission behavior trends, such as similarities of sender domain authentication results and e-mail domains' naming rules.

Finally, we specify clusters which are considered as forwarding servers' clusters. We already know several white forwarders' IP addresses (hereinafter, they are called "known forwarders"). When the cluster has known forwarders, the servers included in this cluster have similarly transmission situation with legitimate known forwarders. Thus, we determine these servers of the cluster as forwarding servers.

IV. Dataset

In this section, we explain the dataset that applies to our method. We utilize DMARC reports that received 31st December 2018 in one of the most famous ISPs' domains in Japan. The number of DMARC reports is 22,305,844, and the number of e-mails including DMARC reports is 232,492,822. In addition, the number of sender's IP address is 536,657.

Figure 3 shows the number of e-mails for each sender's IP address. As shown in Figure 3, top 1% of senders (5,366 IP addresses) based on the total number of e-mails cover about 89.1% of total e-mails in our DMARC reports, which is enough large data to analyze. On the other hand, 99% of senders (531,291 IP addresses) send only a few e-mails in our DMARC reports. In this experiment, we use the DMARC reports from 5,366 (top 1%) servers, excluding the reports from servers with low deliveries. Additionally, these 5,366 servers contain five known forwarders. Thus, we summarize these 5,366 senders' DMARC reports and adapt X-means clustering analysis in our approach.

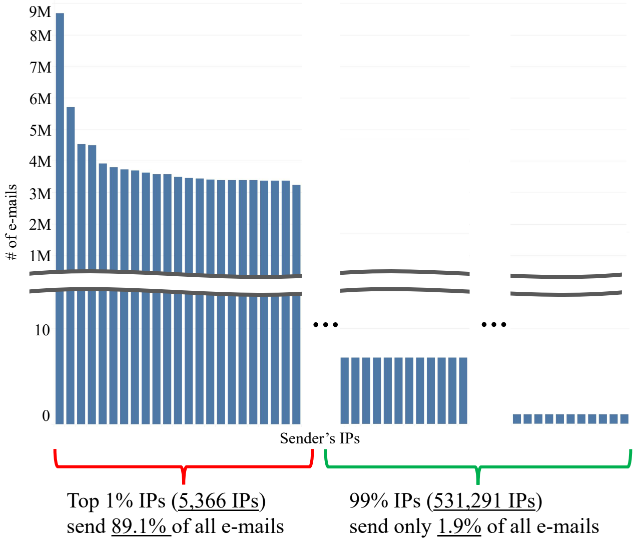

Figure 3. The number of E-mails for each sender's IP address.

TABLE I shows the number of spammer's IP addresses included in our dataset by checking famous IP blacklists ("spamhaus blocklists" [17]) and spam filter results. Spamhaus blocklists are provided by the Spamhaus Project, which is international nonprofit organization tracking spam and related cyber threats. Spam filter results are provided by Japanese famous ISP which is different from DMARC reports provider.

As shown in TABLE I, some spammer's servers are in-

TABLE I. SPAMHAUS AND SPAM FILTER RESULTS OF THE 5,366 IP ADDRESSES.

		Listed	Not Listed
Spamhaus		293 (5.46%)	5,073 (94.5%)
Spam filter	Spam	630 (11.74%)	4,736 (88.26%)
	Ham	1810 (33.73%)	3,566 (66.46%)

TABLE II. THE RESULTS OF APPLYING OUR METHOD TO THE 5,366 IP ADDRESSES.

Clustering Results	#
Clusters	20
Known forwarders	5
Forwarder cluster	1
IP addresses in Forwarder cluster	451

TABLE III. EVALUATION OF FORWARDER CLUSTER IP ADDRESSES UTILIZING SPAMHAUS AND SPAM FILTER RESULTS

	Spamhaus Blocklisted	Spam Filter		# of IPs
		Listed as Spam	Listed as Ham	
1)	True	True	True	0
2)	True	True	False	0
3)	True	False	True	0
4)	True	False	False	0
5)	False	True	True	159
6)	False	True	False	1
7)	False	False	True	196
8)	False	False	False	95

cluded in our dataset applying our method.

V. RESULTS AND EVALUATIONS

In this section, we describe the results of applying our method to our dataset in subsection V-A, and evaluate our approach in subsection V-B.

A. Results of applying our method to DMARC reports

TABLE II shows the results of the clustering. As shown in TABLE II, our method divides 5,366 IP addresses into 20 clusters by X-means clustering analysis. We confirmed that five known forwarders are classified into the same cluster of 20 clusters. Forwarder cluster contains 451 servers, five known forwarders and 446 forwarding server candidates detected by the clustering. Our method determines these 451 servers as e-mail forwarding servers.

B. Evaluation of the clustering results focusing on the forwarder cluster

We evaluate the validity of our approach by analyzing 451 IP addresses. First of all, in order to check whether 451 IP addresses included in forwarder cluster are spammers or not, we compare 451 IP addresses with the spamhaus blocklists and the spam filter results.

As the comparison, we check whether 451 IP addresses are listed in the spamhaus blocklists or not. In addition, we confirm whether 451 IP addresses are listed as spam e-mails sender or ham e-mails sender by using the spam filter results. TABLE III shows all combinations of the evaluation results. For example, the combination 1) in TABLE III shows that no IP address is listed in spamhaus blocklists, listed as spam e-mail, and listed as ham e-mail.

As shown in results 1), 2), 3), and 4) in TABLE III, all 451 IP addresses are not listed in the spamhaus blocklists. This result means that 100% of forwarder cluster's IP addresses are not included in the blocklists.

Then, we describe the comparison results 5), 6), 7), and 8) in TABLE III. 159 IP addresses of 5) in TABLE III send both ham e-mails and spam e-mails in the observation. We can consider that there are two types of transmission behaviors.

The first assumed behavior is that owners of IP addresses are famous E-mail Service Providers (ESPs), ISPs and famous free e-mail services. The spammers often abuse these kinds of IP addresses in order to send malicious e-mails. Therefore, it is obvious that the IP addresses of these providers and services are not spammers' IP addresses. The e-mail accounts hacking is also considered as IP addresses of 5). When the spammers compromise e-mail accounts, the spammers can send spam e-mails utilizing legitimate sender's IP addresses. From these reasons, 159 IP addresses are not spammers' IP addresses although spam e-mails sent from these 159 IP addresses are observed. In addition, 159 IP addresses of 5) are not listed in spamhaus blocklists, therefore these IP addresses are considered as white IP address.

The IP address of 6) sends spam e-mails. This is Japanese application service provider's IP address. This IP address is not spammer's IP address according to spamhaus blocklists, therefore we considered that this IP address is abused by spammers.

196 IP addresses of 7) does not send any spam e-mails. In addition, these IP addresses are not listed in spamhaus blocklists. Thus, we can determine these IP addresses as legitimate senders obviously.

95 IP addresses of 8) does not send both ham e-mails and spam e-mails. In other words, ISP providing spam filter results cannot observe any e-mails from 95 IP addresses of 8). Thus, we cannot determine whether 95 IP addresses are spammers or not by using spam filter results. However, we can consider that these 95 IP addresses are not spammers according to the results of spmahaus blocklists.

To summarize, according to the confirmation results of spam filter results, our approach detected legitimate forwarding server with the accuracy of $\frac{(451-95)-1}{451-95} * 100 \approx 99.72\%$ in the observation of the ISP providing spam filter results.

Next, we show the False Positives that can be reduced by our method. Figure 4 shows the DMARC authentication failure rate of 451 servers classified as legitimate forwarding servers by our method. As shown in Figure 4, amoung the e-mails delivered from each 451 IP addresses, the e-mails with a minimum of 7.9%, a maximum of 74.94%, and a median of 50.17% are failed DMARC authentication. On the other hand, as mentioned above in this section, none of these 451 IP addresses were included in the spamhaus blocklist. Also, from the comparison with the spam filtering result, we confirmed that our method can classify the legitimate forwarding servers with 99.72% accuracy.

From these results, by utilizing the proposed method, e-mail receiving servers can detect 7.9% to 74.94% (median

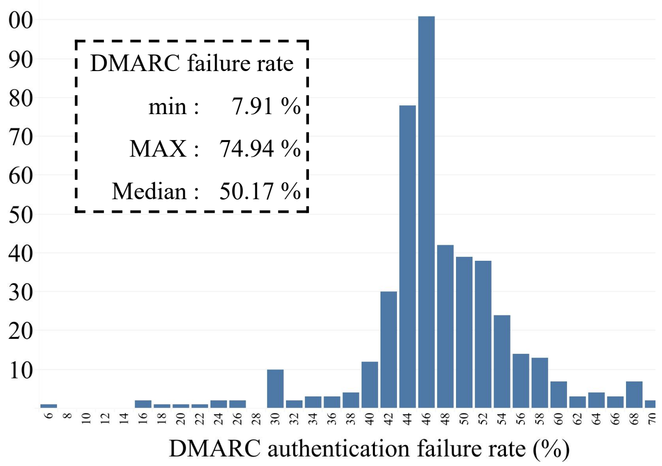

Figure 4. Distribution of DMARC authentication failure rate of 451 IP addresses.

of 50.17%) of legitimate e-mails from each 451 servers that have become False Positives in the conventional DMARC authentication without using heavy loaded spam filter.

VI. Conclusion

In this paper, we proposed a method to detect legitimate forwarding servers by X-means clustering analysis utilizing a large number of DMARC reports data.

In order to classify the legitimate forwarded messages correctly, our approach summarizes DMARC reports focusing on the sender domain authentication results and the e-mail domains at first. In addition, our method classifies the senders' IP addresses by X-means clustering analysis. As a result, we confirmed that the proposed method can classify transfer servers with high accuracy. Thus, when e-mail server administrators know a few forwarding servers, such as the servers in their own organization beforehand, they can detect many other legitimate forwarders by utilizing our method.

In our approach, the sender's IP addresses are classified based on their transmission behavior. Although we focus on one forwarding IP addresses cluster, we consider that other clusters have similarity of transmission behavior each other. Thus, in order to detect forwarding server or spammer's server in higher accuracy, analyzing other clusters' e-mail sending behavior is future subject.

In addition, we consider that our clustering results can utilize the model of forwarding servers' transmission behavior. By modeling forwarders' transmission behaviors, we can improve the accuracy to detect legitimate forwarding servers. Therefore, modeling our clustering results is also future subject.

Acknowledgment

This study was supported by TwoFive Inc. through a collaborative research project.

References

[1] FBI (Federal Bureau of Investigation), "Public Service Announcement, Business E-mail Compromise The 12 billion dollar scam," 2018, URL: https://www.ic3.gov/media/2018/180712.aspx [Accessed: 15th May. 2019].

[2] M. Wong and W. Schlitt, "Sender Policy Framework (SPF) for authorizing use of domains in e-mail," RFC4408, Tech. Rep., 2006.

[3] D. Crocker, T. Hansen, and M. Kucherawy, "DomainKeys Identified Mail (DKIM) signatures," STD76, Tech. Rep., sep 2011.

[4] M. Kucherawy and E. Zwicky, "Domain-based message authentication, reporting, and conformance (DMARC)," RFC 7489, Tech. Rep., 2015.

[5] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, G. Paliouras, and C. D. Spyropoulos, "An evaluation of Naive Bayesian anti-spam filtering," Proceedings of the workshop on Machine Learning in the New Information, 2000, pp. 9–17.

[6] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, and C. D. Spyropoulos, "An experimental comparison of naive Bayesian and keyword-based anti-spam filtering with personal e-mail messages," Proceedings of the 23rd annual international ACM SIGIR conference on Research and development in information retrieval, 2000, pp. 160–167.

[7] S. Aggarwal, V. Kumar, and S. D. Sudarsan, "Identification and detection of phishing emails using natural language processing techniques," in Proceedings of the 7th International Conference on Security of Information and Networks. ACM, 2014, p. 217.

[8] H. Ducker, D. Wy, and V. N. Vapnik, "Support vector machines for spam categorization," IEEE Transactions on Neural networks, vol. 10, no. 5, 1999, pp. 1048–1054.

[9] W. Feng, J. Sun, L. Zhang, C. Cao, and Q. Yang, "A support vector machine based naive Bayes algorithm for spam filtering," in Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International. IEEE, 2016, pp. 1–8.

[10] T. S. Guzella and W. M. Caminhas, "A review of machine learning approaches to spam filtering," Expert Systems with Applications, vol. 36, no. 7, 2009, pp. 10 206–10 222.

[11] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. A. Najada, "Survey of review spam detection using machine learning techniques," Journal of Big Data, vol. 2, no. 1, 2015, p. 23.

[12] "The Apache SpamAssassin Project," URL: http://spamassassin.apache.org/ [Accessed: 15th May. 2019].

[13] J. Mason, "Filtering spam with spamassassin," In HEANet Annual Conference, 2002.

[14] S. Sinha, M. Bailey, and F. Jahanian, "Shades of Grey: On the effectiveness of reputation-based "blacklists"," in 3rd International Conference on Malicious and Unwanted Software (MALWARE). IEEE, 2008, pp. 57–64.

[15] C. J. Dietrich and C. Rossow, Empirical research of ip blacklists. Springer, 2009, pp. 163–171.

[16] D. Pelleg and A. Moore, "X-means: Extending K-means with Efficient Estimation of the Number of Clusters," in Proceedings of the 17th International Conference on Machine Learning. Morgan Kaufmann, 2000, pp. 727–734.

[17] The Spamhaus Project Ltd., "Spamhaus ZEN," URL: https://www.spamhaus.org/zen/ [Accessed: 15th May. 2019].