2019 International Computer Science and Applications Conference (ICSAC 2019)

A Hybrid Privacy Preserving against Multi-attacks for Network Data Publication

Jianmei Cao
State Grid of China Technology College,
Jinan, China

Xianglai Yang
State Grid of China Technology College,
Jinan, China

Youjie Wang
State Grid of China Technology College,
Jinan, China

***Abstract*—Network trace data provides valuable information which contributes to model network behavior, defends network attacks, and develops new network protocols. Therefore, releasing network trace data is highly demanded by researchers and organizations to promote development of network technologies. However, due to the sensitivity of the network track data, it is a potential risk for organizations to publish the original data which may expose their commercial confidentiality and customers' privacy within their networks. Several methods have been proposed to prevent network track attacks, such as statistical fingerprinting and injection. Unfortunately, they are not sufficient to protect privacy because adversary can use more background knowledge to reach the intended attack, and this kind of attack is proved to be used. This paper proposed an attack model named Multi-Attacks by using more background knowledge. For this attack model, it extracts the inherent graphics structure between the source and destination IP addresses in the network trace data and proposes a solution, data swapping, to prevent the target host from being recognized, which is based on k-anonymity. Combined with other protection techniques, our method can effectively prevent this Multi-Attacks model while preserving the data utility and providing formal guarantees of confidentiality protection. And using data swapping method for privacy protection can provide a more perfect solution, reach a higher level of privacy protection and guarantee good data utility related to the anonymity-based approach. Lastly, our proposed algorithm is applied to different real datasets and demonstrate its effectiveness over several existing network trace data anonymization techniques.**

Keywords—network trace data, fingerprinting, injection, k-anonymity, data swapping

I. INTRODUCTION

In recent years, an explosive increasing in network trace data has been made publicly available and it can be freely collected by different organizations for various purposes. This data contains a lot of significant information which could promote the development of network and data science, for example it could be analyzed by network researchers to modeling the network behaviors, defensing network attacks and developing new protocols. However, it is also risky for organizations to publish the original data. For instance, by analyzing the publishing network data, the attackers could know the IP addresses the target host have visited, then he may infer more sensitive information such as the service type of a server, some individual privacy of a user such as religious belief, health condition, family address, and the privacy of other users whom he has connected to. By analyzing the published network data, an attacker could obtain information about the structure of the network, so he may infer the bottleneck in the target network which will contribute to carry out a more effective DDOS attack. In order to protect the sensitive information not be disclosed while keeping the data utility, several approaches have been proposed. Those methods mainly focused on encrypting the IP address and modifying the packet's header data, whereas both of them are not only vulnerable to attack, but also lead to poor data utility.

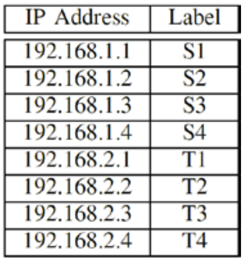
This paper proposes a new attack model, called Multi-Attacks. This attack model is considered to combine the current more popular attacks and has a higher attack efficiency. We take into account this attack model exploiting the bipartite graph constructed over IP addresses in network trace data. In the bipartite graph, the IP addresses are vertices, the correspondence inside a pair of source and destination IP addresses is an edge. If an attacker identifies a communication (i.e., an edge in the graph), then the attacker can identify two hosts (i.e., vertices) within the network trace (i.e., the graph)[14]. That is, the more edges about the target internal vertex in the graph the attacker identifies, the higher probability he has to identify the target vertex, even he may uniquely determine it. The attacker might also have prior information about the target hosts such as some IPs that the target host has contacted, or he may inject some flows to the target network which could effectively help him to carry out this attack. In order to resist this Multi-Attacks model, we proposed to use a data swapping algorithm with k-anonymity principle to prevent the target hosts from being identified with the probability more than 1/k. In addition, when the parameter k is turned to a suitable value, the method we proposed can be proved to completely defense the Multi-Attacks model. And the publisher can adjust parameter k to get a higher level of protection or remain a better data utility.

The organization of the rest of this paper is structured as follows. In section II, we give the preliminaries and notations, problem definition, adversary model and the information loss metrics used in this paper. In section III, we propose models and algorithms based on an idea of data swapping. In section IV, we analyze the properties of the dataset and illustrate the experimental evaluation. Finally, we present the conclusions and the future work in section V.

II. PROBLEM STATEMENT

A. Preliminaries and notations

The IP address of all data is divided into internal IP and external IP, there is a communication record between the internal IP and the external IP, but there is no communication record between the internal IP. This constitutes a bipartite graph structure. If using the number of interactive packets between two IPs as a weight, then it constitutes a weighted bipartite graph, the protection program is built on the graph structure. We use *G=(V,E,W)* to represent the bipartite graph, vertex V represents the internal and external IP address, edge E indicates whether there is a communication between the internal vertex and the external vertex, the weight W represents the number of packets interacted between internal vertex and external vertex. What the sensitive attribute we want to protect is the host's IP address and the communication between the internal IP and the external IP. Then corresponding to the k-anonymity model principle, the IP address is regard as the identifier, and the external IP connected to the internal IP is regard as the quasi-identifier, and also as a sensitive attribute needs to be protected. Suppose that Fig. 1 is the label of IP, 192.168.1.1~192.168.1.4 as the source IP address set and 192.168.2.1~192.168.2.4 as the destination IP address set. The edge's weight is the number of packets. It can be extracted structure as shown in Fig. 2.



IP Address	Label
192.168.1.1	S1
192.168.1.2	S2
192.168.1.3	S3
192.168.1.4	S4
192.168.2.1	T1
192.168.2.2	T2
192.168.2.3	T3
192.168.2.4	T4

Fig. 1. IP LABELING

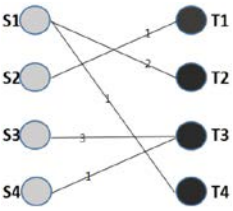


Fig. 2. Graph structure of table 1

B. Problem Definition

We denote by G an original set of network flows, and by G* the anonymized version of G released by the publisher. The fields of the flows include a confidential multi-value attribute $A^p = \{src\_ip, dst\_ip\}$, and a set of other fields $A^i = \{A_1, A_2, \ldots, A_m\}$ that may be used to infer A^p, where these attributes can be used as Quasi-Identifier. In particular, some flow fields may be exploited to identify A^p based on the hosts' characteristics. Here, we give the formal definitions of the Multi-Attacks model we proposed.

Definition 1. (Multi-Attacks) This paper gives the attacker more background knowledge, proposes an attack model named Multi-Attacks. This attack model combines at least two of the three attack modes of "injection attack", "fingerprinting attack", and "edge attack" so that it can improve the efficiency of the attack. We are formally defined as $A = C_3^{2,3}\{a_1, a_2, a_3\}$. Where A represent the Multi-Attacks model, a_1, a_2, a_3 respectively represent injection attack, fingerprinting attack and edge attack. $C_3^{2,3}\{a_1, a_2, a_3\}$ means selecting two or three combinations of attacks. If combined with three attacks, it will greatly enhance the ability of the attacker.

C. Adversary Model

For the released data G*, the goal of the adversary is to recover the encrypted data, identify the target host t and get more information of it. The considered adversary model is based on the following assumptions.

1) The adversary may observe G*.

2) The adversary may know in advance where and when the flows will be collected, and may inject some flows to the target network.

3) The adversary may have prior information about the target host and know some IPs that the target host has contacted, which can help adversary to know the edge's weight in original data G.

4) The adversary may simulate the target network status and know the fingerprint of target host, and he may also know the fingerprints of the destination host that the target host has contacted, which acts as the Quasi-Identifier of the edge attribute.

D. Metrics for information loss

For the solution we proposed, three types of information loss metrics methods are used, including general metrics, statistical metrics and our metrics.

Our Metrics: We need to define a dedicated metric to represent the change. Suppose |E| is the total number of edges and |W| is the total weight in the IP-weighted bipartite graph. In our method, we will add and delete some edges of the IP-weighted bipartite graph, and also add and delete corresponding weights of it, which means adding and deleting records of original data. The metrics to reflect the graph change are the Ratio of Adding Edges(RAE), the Ratio of Deleting Edges(RDE), the Ratio of Adding Weight(RAW), the Ratio of Deleting Weight(RDW) which are defined as (5)~(8):

All the methods of developing an IP mapping or shifting the edges of the IP-graph will involve a problem of changing the original corresponding relation of source IP and destination IP. In our method, we will remain the edges that are non-sensitive, and shift the sensitive edges of the IP-weighted bipartite graph, and also remain and shift the corresponding weights. Suppose |E| is the total number of edges and |W| is the total weight in the IP-weighted bipartite graph. The metrics to reflect the graph change are Ratio of Change Edges (RCE) and Ratio of Change Weight (RCW), which are defined as Equation (1) and (2).

$$RCE = \frac{|cE|}{|E|} \tag{1}$$

$$RCW = \frac{|cW|}{|W|} \tag{2}$$

In which, |cE| is the total changed edges, |cW| is the corresponding changed weights which represents the number of changed record. These metrics will be used to represent how much the graph is changed. The less these values are, the better utility the anonymized data could have. RCE also means an attacker could infer an edge is true with the probability of 1-RCE. That is, the higher RCE is, the harder for an attacker to recognize an edge.

In our method, some edges may need to be suppressed, so we use the Ratio of Suppressed Edges (RSE) and Ratio of Suppressed Weight (RSW) to reflect our method's utility, which are defined as Equation (3) and (4).

$$RSE = \frac{|sE|}{|E|} \quad (3)$$

$$RSW = \frac{|sW|}{|W|} \quad (4)$$

In which, |sE| is the total suppressed edges, |sW| is the corresponding suppressed weights which represents the number of suppressed records.

III. Data Swapping-based Method

In our proposed method, we take the same way to construct weighted bipartite graphs. This method combines the data swapping technology and the anonymization technology to propose a more effective privacy protection algorithm, and the information loss is very low in many aspects. Using data swapping method for privacy protection, it can provide a higher level of privacy protection and a good guarantee of data availability related to the anonymous-based approach.

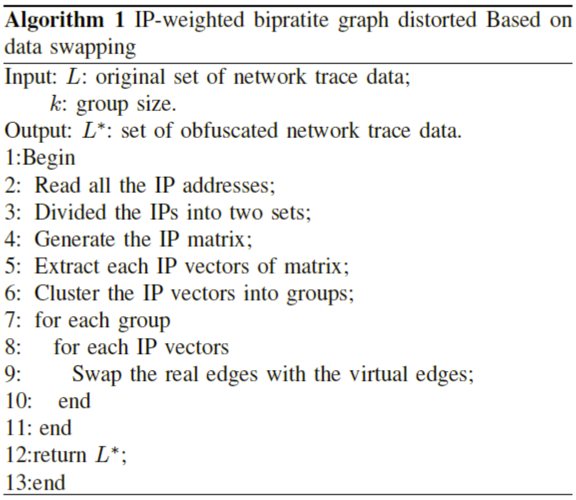
In order to better defense Multi-Attacks model, we can group the internal IPs that have similar connections to the external IPs. Our method is described as Algorithm 1. The basic steps are shown as follows:

The first three steps of the algorithm are to divide IPs into two sets, generate IP matrix, and cluster IP vectors into groups. These three steps are the same as the first method based on k-anonymity, so we will not repeat them here. The next will introduce the core of the algorithm, that is, data swapping.

A. Swap the real edges with the virtual edges

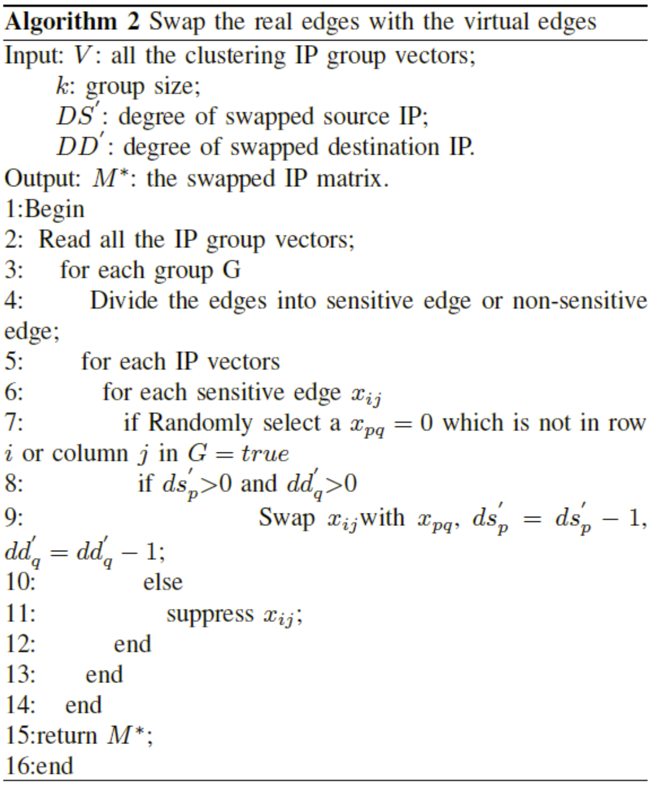
Data Swapping method is described as Algorithm 2. In the IP matrix M_{n*m}, if $x_{ij} \neq 0$,, we consider there is a real edge between i and j. if $x_{ij} = 0$, there is no edge between i and j. However, to facilitate describing our swapping method, we name the latter virtual edge. We will swap the real edges with the virtual edges to change the original mapping relation. In fact, not all the real edges need to be swapped because some edges will not contribute to identify the target based on our method, so these edges will maintain the original mapping relation. In each group G_i, we abstract the sub matrix $s\ M_i$ of the total IP matrix M_i, then we define which edge in $s\ M_i$ the is sensitive edge or non-sensitive edge (line 4).

Group of non-sensitive edges: For the $s\ M_i$ of group G_i, if all the value of a column j is non-zero, we consider the column is a group of non-sensitive edges.



Algorithm 1 IP-weighted bipratite graph distorted Based on data swapping

```
Input: $L$: original set of network trace data;
    $k$: group size.
Output: $L^*$: set of obfuscated network trace data.
1:Begin
2:  Read all the IP addresses;
3:  Divided the IPs into two sets;
4:  Generate the IP matrix;
5:  Extract each IP vectors of matrix;
6:  Cluster the IP vectors into groups;
7:  for each group
8:      for each IP vectors
9:          Swap the real edges with the virtual edges;
10:     end
11: end
12:return $L^*$;
13:end
```

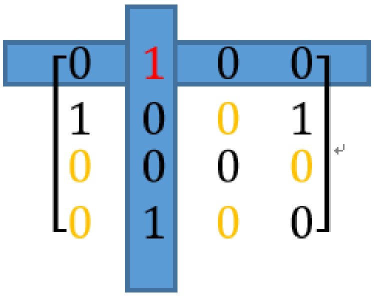


Algorithm 2 Swap the real edges with the virtual edges

```
Input: $V$: all the clustering IP group vectors;
    $k$: group size;
    $DS'$: degree of swapped source IP;
    $DD'$: degree of swapped destination IP.
Output: $M^*$: the swapped IP matrix.
1:Begin
2:  Read all the IP group vectors;
3:    for each group G
4:        Divide the edges into sensitive edge or non-sensitive edge;
5:        for each IP vectors
6:            for each sensitive edge $x_{ij}$
7:                if Randomly select a $x_{pq} = 0$ which is not in row $i$ or column $j$ in $G = true$
8:                    if $ds'_p$>0 and $dd'_q$>0
9:                        Swap $x_{ij}$with $x_{pq}$, $ds'_p = ds'_p - 1$, $dd'_q = dd'_q - 1$;
10:                   else
11:                       suppress $x_{ij}$;
12:               end
13:           end
14:   end
15:return $M^*$;
16:end
```

To maintain the degree distribution of each node, before swapping the edges, we define degree of internal IP $DS = \{ds_1, ds_2, \dots, ds_n\}$ and degree of external IP $DD = \{dd_1, dd_2, \dots, dd_n\}$ to record the degree distribution. We also randomly swap the degree of nodes in DS and DD. Suppose the swapped degree is $DS = \{ds'_1, ds'_2, \dots, ds'_n\}$ and $DD = \{dd'_1, dd'_2, \dots, dd'_m\}$, we can use them to control the swapping process. If we swap the real edge x_{ij} with the virtual edge x_{pq}, the current degree of node p and q need plus 1. The degree of the node can not be greater than his corresponding ds' and dd', which means if the degree of internal IP node i is greater than or equal to ds'_i, the edges of node i need not be swapped, and the *ith* row need not be changed; if the degree of external IP node j is greater than or equal to dd'_j, the edges of node j need not be swapped, and the *jth* column need not be changed.

We also add a swapping rule to ensure that the two nodes of an edge will be both changed in each set: If the real edge x_{ij} need to be swapped, it can not be swapped with the virtual edge in the *ith* and *jth* column of M_{n*m}. For example, in Fig 3, we want to swap the real edge x_{12} (colored by red) to a virtual edges where the $x_{ij} = 0$. The 0 in row i=1 and column j=2 can not be swapped with x_{12}. Otherwise either source IP or destination IP will remain unchanged, and the 0 on diagonal are also could not be swapped because it is meaningless to make diagonal element 1. So the 0 could only be swapped with one of $x_{23}, x_{31}, x_{34}, x_{41}, x_{43}$ (colored by yellow). However, this will limit our method to process only a data set which satisfies $\mathrm{E} \leq \mathrm{n} * \mathrm{m}/2$. Because there is only a relatively sparse matrix with sufficient 0 can be easily satisfy the exchange conditions. So we will swap the edges according to this rules (line 5~13). If there is not any appropriate 0 to be swapped with x_{ij}, we will suppress it (line 10).



$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Fig. 3. Example of edge swapping

B. Encrypt the IPs

The IP address itself is not sensitive information, while when it is linked with a host, it is. So we also need to disguise the value of it. There are too many methods to encrypt the IP address, we can use any of them like Crypto-PAn or an easier method. However, it is also feasible not to encrypt the IP address value, because under our method, the attacker cannot get the real mapping information beyond the probability of 1/k .

C. Modify the original data set

After the above steps, we just need to modify the original data set according to the new mapping relationship.

D. External

According to the above method we can see, when we set the parameter k to n, our method could completely defend the Multi-Attacks model. While our approach may change all edges, we do not need to change other header information except IP, this can be considered to maintain great data availability.

IV. EXPERIMENTS

A. DataSets

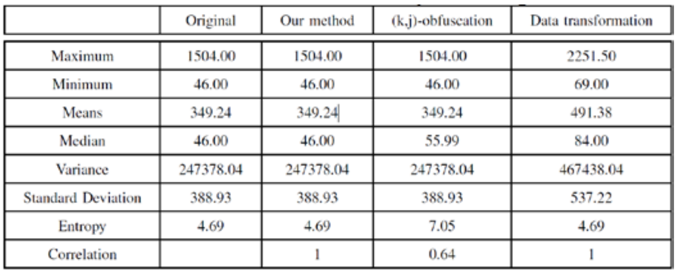
We use two data sets for our experiments. Data set 1 is downloaded from www.caida.org. We collect the data from the data set “Anonymized Internet Traces 2016” which contains anonymized passive traffic traces from CAIDA’s equinix-chicago monitor on high-speed Internet backbone links. The data set is too large to process, so we select a small part of it which is easier for us to deal with. We choose 9,630 packet header records with 100 internal IPs and 100 external IPs. Data set 2 is the 1998 Testing Data - Week 1-MondayTcpdump of the Lincoln Laboratory[5]. The 118,695 records contain 725 different IPs which can be divided into two groups, one contains 698 IPs (internal) and another contains 27 IPs (external).

B. Results and Analysis

In data set 1, we set the values of k varying from 2 to 20, while in the data set 2 k varies from 2 to 100. We apply the sparse subspace clustering algorithm on data set 1 while not on data set 2, because the IP matrix’s dimension is high in data set 1 but not in data set 2. It is worth noting that the parameter k we set is the anonymity parameter but not the number of clusters of the k-means algorithm. Due to the initial points’ uncertainty of the k-means algorithm, the result of each running is different, so we run the algorithm for 100 times and calculate the average value of each attribute.

(1) Results and Analysis Based on data swapping Method

Statistics characters of packet header information: Fig 4 shows the comparison in statistics characters. We can see both the (k,j)-obfuscation[11] and data transformation [9] have changes on Mean, Median, Variance, Standard Deviation. And (k,j)-obfuscation also has a change on Correlation and Entropy, while data transformation has changes on Maximum and Minimum. And the amount of changes for these methods is related to the parameter k in (k,j)-obfuscation and in data transformation, while our method could maintain all the characters.

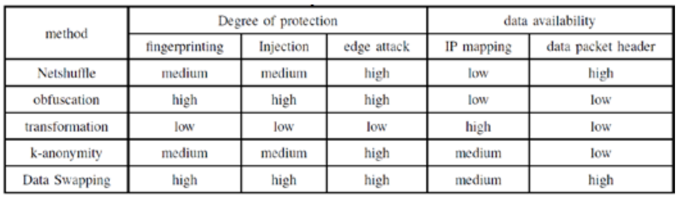


	Original	Our method	(k,j)-obfuscation	Data transformation
Maximum	1504.00	1504.00	1504.00	2251.50
Minimum	46.00	46.00	46.00	69.00
Means	349.24	349.24	349.24	491.38
Median	46.00	46.00	55.99	84.00
Variance	247378.04	247378.04	247378.04	467438.04
Standard Deviation	388.93	388.93	388.93	537.22
Entropy	4.69	4.69	7.05	4.69
Correlation		1	0.64	1

Fig. 4. Statics characters of packet length

(2) Comparison of various methods

Fig 5 shows a comparison of the representative methods in recent years with the approach presented in this paper. It can be seen that the Netshuffle method has a good balance between privacy and data availability. And (k,j)-obfuscation provides a high level of privacy protection, but it also has a high loss of information. Our data swapping based approach provide a higher level of privacy protection while keeping a good guarantee of data availability. Data transformation in terms of degree of protection and data availability are not as good as other methods. The method proposed in this paper have their merits, in general, is superior to the existing method.



method	Degree of protection			data availability	
	fingerprinting	Injection	edge attack	IP mapping	data packet header
Netshuflle	medium	medium	high	low	high
obfuscation	high	high	high	low	low
transformation	low	low	low	high	low
k-anonymity	medium	medium	high	medium	low
Data Swapping	high	high	high	medium	high

Fig. 5. Comparison of methods

V. CONCLUSION

In this paper, we review the previous anonymization technique and the kinds of common attacks to the network trace data and proposed a more aggressive Multi-Attacks model. For this attack model, we apply data swapping technique to the weighted bipartite graph constructed on the mappings between the internal and external IP addresses, and proposed a solution to prevent this attack on the release of network data. Under the protection of our method, the probability of the attacker to identify the target host or any other useful information is at most 1/k. Our main contribution is to use the graph distortion based on k-anonymity on the IPs mapping to prevent internal IPs from being identified under the Multi-Attacks model. Through the process of graph distortion, we can achieve indistinguishable IP-vertexes, which means any group after the process of anonymity has at least k indistinguishable IP-vertexes, and the probability of identifying the target host is at most 1/k. Our method is proved to defense this attack when the parameter k is tuned to a suitable value. Two data sets of different sizes used in our experiments show that our methods are feasible, it can protect the IP addresses while maintaining an acceptable level of data utility. For the privacy preserving of the released network data, there are several future research directions, for example how to apply anonymous technology from general structure data to network data, how to define the privacy protection model of network data, and how to balance the privacy and data utility. There is no uniform conclusion to solve these three problems, which is the future work needs to be addressed.

REFERENCES

[1] Brekne, T., Rnes, A., Arne: Anonymization of ip traffic monitoring data: attacks on two prefix-preserving anonymization schemes and some proposed remedies. In: International Workshop on Privacy Enhancing Technologies. pp. 179–196 (2005)

[2] Burkhart, M., Schatzmann, D., Trammell, B., Boschi, E., Plattner, B.: The role of network trace anonymization under attack. Acm Sigcomm Computer Communication Review 40(1), 5–11 (2010)

[3] Coull, S.E., Wright, C.V., Monrose, F., Collins, M.P., Reiter, M.K.: Playing devil's advocate: Inferring sensitive information from anonymized network traces. In: Network and Distributed System Security Symposium, NDSS 2007, San Diego, California, Usa, February - March. pp. 35–47 (2007)

[4] Fan, J., Xu, J., Ammar, M.H., Moon, S.B.: Prefix-preserving ip address anonymization: measurement-based security evaluation and a new cryptography-based scheme. Computer Networks 46(2), 253–272 (2004)

[5] Foukarakis, M., Antoniades, D., Polychronakis, M.: Deep packet anonymization. In: European Workshop on System Security. pp. 16–21 (2009)

[6] Harvan, M., Schonwalder, J.: Prefix- and lexicographical-order-preserving ip address anonymization. In: Network Operations and Management Symposium, 2006.

[7] NOMS 2006. Ieee/ifip. pp. 519–526 (2006)

[8] Koukis, D., Antonatos, S., Antoniades, D., Markatos, E.P.: A generic anonymization framework for network traffic. In: IEEE International Conference on Communications. pp. 2302–2309 (2006)

[9] Lakhina, A., Crovella, M., Diot, C.: Diagnosing network-wide traffic anomalies. In: Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. pp. 219–230 (2004)

[10] Mivule, K., Anderson, B.: A study of usability-aware network trace anonymization. In: Science and Information Conference. pp. 1293–1304 (2015)

[11] Pang, R., Allman, M., Paxson, V., Lee, J.: The devil and packet trace anonymization. Acm Sigcomm Computer Communication Review 36(1), 29–38 (2006)

[12] Riboni, D., Villani, A., Vitali, D., Bettini, C.: Obfuscation of sensitive data in network flows. In: INFOCOM, 2012 Proceedings IEEE. pp. 2372–2380 (2012)

[13] Seeberg, V.E., Petrovic, S.: A new classification scheme for anonymization of real data used in ids benchmarking. In: International Conference on Availability, Reliability and Security. pp. 385–390 (2007)

[14] Slagell, A., Lakkaraju, K., Luo, K.: Flaim: a multi-level anonymization framework for computer and network logs. In: Conference on Large Installation System Administration. pp. 6–6 (2006)

[15] Valgenti, V.C., Paul, R.R., Min, S.K.: Netshuffle: Improving traffic trace anonymization through graph distortion 41(4), 1–6 (2011)

[16] Yen, T.F., Huang, X., Monrose, F., Reiter, M.K.: Browser fingerprinting from coarse traffic summaries: Techniques and implications. In: Detection of Intrusions and Malware, and Vulnerability Assessment, International Conference, DIMVA 2009, Como, Italy, July 9-10, 2009. Proceedings. pp. 157–175 (2009)