# A Behavior-based Method for Detecting DNS Amplification Attacks

Cai, Longzhu
Kyushu University

Feng, Yaokai
Kyushu University

Kawamoto, Junpei
Kyushu University

Sakurai, Kouichi
Kyushu University



出版情報：Proc. of the 10th International Workshop on Advances in Infromation Security, pp.1-, 2016-07-06
バージョン：
権利関係：

# *A Behavior-based Method for Detecting DNS Amplification Attacks*

Longzhu Cai, Yaokai Feng, Junpei Kawamoto, Kouichi Sakurai
Kyushu University
Department of informatics, Sakurai Laboratory
744 Motooka, Nishi-ku, Fukuoka 819-0395, JAPAN
2IE15016G@s.kyushu-u.ac.jp
fengyk@ait.kyushu-u.ac.jp,{kawamoto,sakurai}@inf.kyushu-u.ac.jp

***Abstract*—DNS (Domain Name System) amplification attack has become a popular form of the attacks of the Distributed Denial of Service (DDoS) in recent years. In DNS amplification attacks, the attackers utilize spoofed source IP addresses and open recursive DNS servers to perform the bandwidth consumption attacks. A lot of responses are generated and they are sent to the targets after the attackers send only a little of DNS requests. Various methods have been proposed for detecting the DNS amplification attacks. However, almost of them have to determine parameters in advance, which is not easy for many cases. In this study, we utilized the detection pattern and combination of three features to distinguish normal and attack. It can solve the problem that limitation of detection in the case of high-frequency and low-amplification attack.**

***Keywords—DNS; amplification; DDoS; detection; k-means***

## I. INTRODUCTION

In March 2013, the non-profit organization Spamhaus has been suffered a serious cyber attack. This organization called Spamhaus is providing services like filtering spam mail for a lot of users. Because of attack, Spamhaus's server was down and lead to the inbox of users were filled with a lot of spam emails. At that time, the attack method used by the attacker was DNS (Domain Name System) amplification attack.

DNS amplification attack is a method of attack that consumes resource of the network. Currently, a number of open resolver servers on the network have been used to amplifiers frequently by attackers.

Currently, many of the DNS servers have EDNS (Extension Mechanism for DNS) function [1]. The response of DNS packet can be transmitted on the UDP by this mechanism even the size of the packet exceeds 512 bytes. Originally EDNS is made to bring benefits to the users, but now it is often abused to perform DNS amplification attack. Moreover, DNSSec eliminates the possibility of DNS cache-poisoning attacks [2][3], but has been criticized for potentially increasing the probability of DNS DDoS attacks [4][5].

There are research works towards the DNS amplification attacks [6][7]. They have been proposed to take measures with a variety of detection methods. However, there is a problem of the low general versatility of the detection. In other words, conditions and performance of the DNS servers are different, so there is a possibility that some optimized detection method for a server may not be exhibited the same effect in other environments.

On considering these questions, our detection method utilizes the detection pattern learned from historical data of the monitored network and three features to distinguish between normal and abnormal time period on the DNS server. The three features used in our proposal are the frequency of DNS request, rate of amplified data traffic in a time period (response traffic/request traffic) and amount of increased packet in a time period.

## II. MECHANISM OF DNS

### A. About DNS

DNS protocol is popular among attackers to abuse for denial-of-service attacks. Because DNS protocol is basically using the UDP (User Datagram Protocol). And the UDP protocol has high transfer efficiency in a connectionless protocol since small delay. It is often used in applications that focus on high-speed and immediacy. However, it is pointed out that UDP is less reliable than the TCP (Transmission Control Protocol) that connection-oriented protocol. The attackers are usually utilizing such drawbacks of the UDP protocol.

First, we want to explain briefly about DNS searches for DNS requests including recursive search and iterative search [8]. In our explanation, "dns.example.com" is used as an example.

### B. Recursive search

As shown in Fig.1, the recursive search consists of the following steps.

- A name resolution request is sent to the local server from the client side.
- The local server looks for records from the cache server. If such records exist, then send a response. If not, then send a message to the root DNS server.
- After receiving the request, root server transmits the address of the top DNS server that corresponding to the ".com" domain name to the local server.

- The local server is also sending a name resolution request to the ".com" top DNS server.
- ".com" Top DNS server looks for a corresponding from the cache server. If it is found, sending a response. If it does not exist, sending an address of the DNS server corresponding to the ".example.com" domain name to the local server.
- Repeat.

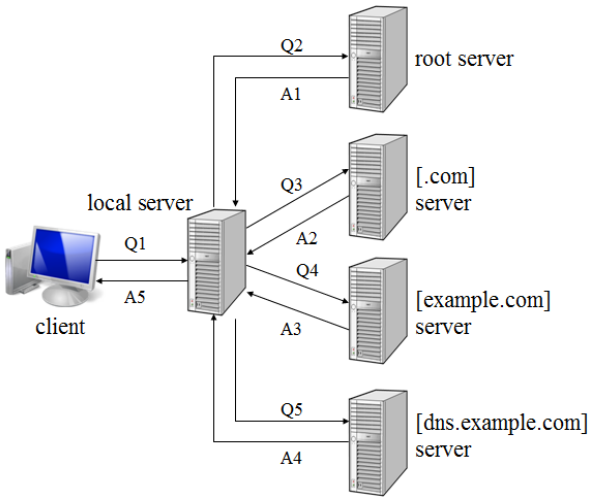


Fig.1 Example of recursive search.

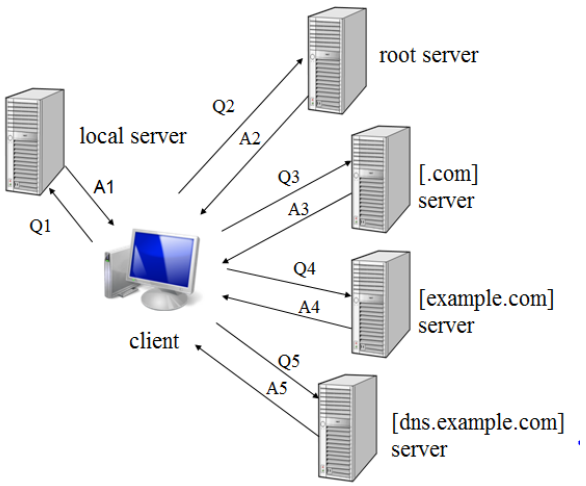


Fig.2 Example of iterative search [9].

### C. *Iterative search*

As shown in Fig.2, the search consists of the following steps.

- A name resolution request is sent to the local server from the client side.
- The local server looks for records from the cache server. If such records exist, then send a response. If not, then send information about the address of root DNS server and response packet to the client.
- After receiving the response, a client will send a request to the root DNS server.
- After receiving the request, root DNS server transmits the address of the DNS server that corresponding to the ".com" domain name and response packet to the client.
- Repeat.

## III. DNS AMPLIFICATION ATTACK

DNS amplification attack is one kind of the reflection attacks, which makes use of the cache function of DNS server [10].

### *Flow of DNS amplification attack*

Generally, those computers or services which called DNS server have two functions. An authoritative name server is a name server that gives answers in response to requests asked about names in a zone. And caching name servers store DNS query results for a period of time determined by the configuration of each domain name record. The flow of DNS amplification attack is as follows.

- The attacker uses a malware to invade authoritative name server having vulnerabilities on the Internet and registering a large-size file. Or the attacker can set up a server that has the same function as the authoritative name server on his own.
- The attacker uses a large number of zombie PCs that infected with remote management malware in advance to send record queries to the caching name server at the same time. (Zombie PC is a vulnerable computer that has been invaded by attacker.)
- Caching nameserver sends a request to the authoritative name server.
- Caching nameserver obtains the above-mentioned large-size registration file from the authoritative nameserver.
- The attacker uses spoofed ID to sending record queries.
- Then a large-size record information is sent to the victim's side from caching nameservers. In this way, the victim network becomes congested and resulting in a down because of overload.

## IV. OUR STUDY

In our study, we extract the number of requests, amplification multiple of data traffic (response traffic size /request traffic size) and simulate amplification multiple of the number of packets (the number of response packet/the number of request packet) per unit time from historic data. Using these data we propose a method to identify the distribution area of the DNS amplification attack by using pattern identification.

In our work, we use the above-mentioned three features to determine the detection pattern. Now, let's see the reason why we use these three features. In DNS amplification attacks, the

attacker utilizes a number of zombie PCs to send a large number of requests to the DNS server that used as an amplifier at a specific time. Therefore, the DNS server that used as step ladder will undergo numerous requests than usual. So, we think the fact that frequency of the requests increases greatly can be used as one of the important features. In addition, by a number of inquiries, the amount of data (in bytes) in one unit time also increase greatly during the attacks. From the basic fact that the response packet corresponding to a request sent from a zombie PC is very large, the expansion rate of the data traffic size from request to response can be used to detect DNS amplification attacks. According to our investigations, we found that only the above two features may be not enough. This is because that, in order to avoid being detected, the attackers possibly send the requests with a little or no change in the expansion rate of the traffic data size. Thus, in this study, the ratio of the number of the reply packets to that of request packets in one unit time is used as the third feature. In this paper, in order to explain the role and necessity of the third feature, simulation experiment is performed twice. As a result, not only detection precision is increased, but also determining the real-time data being normal and abnormal (attack) become easier, which just need calculating the distance from real-time data to the reference point. Moreover, it is no longer necessary to record the IP address of each packet.

### *A. Simulation experiment*

Utilizing two or three features and k-means clustering method to make detection pattern. In the detection pattern, there are several groups, each of which is determined normal or abnormal. And whether an instance is normal or abnormal is determined by its distance from the reference point of each group (the reference point will be described in Fig.5). And we compared the results of two simulation experiments (two or three features being used).

### *B. Detection pattern*

As shown in Fig.3, X-axis is the number of requests per unit time, Y-axis is the ratio of the response traffic to request traffic. Because DNS amplification attack is primary to expand the size of the response record, so the expanding rate is often high. Thus, by clustering the historic data, the abnormal pattern can be found out.

An example was shown in Fig.3. The low-left point is a reference point of the normal group, and the upper-right point is a reference point of the abnormal group. For a new data, we can use a clustering method to determine it is normal or abnormal. And at experiment II, we calculate the distance of between data and every reference to determine the data should be divided into which group.

In this paper, two groups of detection pattern: normal and abnormal are created by using k-means method.

### *C. K-means algorithm*

The K-means algorithm can be described as follows.

- Select reference point $v_1, v_2, \ldots, v_k$.
- Calculate the distance of data to every reference point and put it into the cluster that closer to it.
- Calculate the reference of each cluster again.
- Repeat until satisfied convergence condition.

In this paper, we use the Euclidean distance in the k-means algorithm.

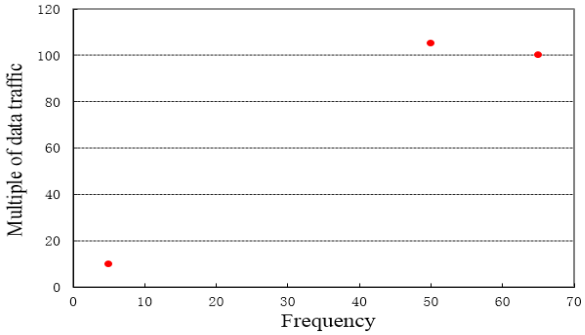


Fig.3 Preliminary experiment.

## V. EXPERIMENT I

As described above, detection based on the frequency of requests and amplification of the traffic passing through the DNS servers in every unit time. Using these two features, normal and abnormal can be classified by k-means algorithm.

### *A. Experiment dataset*

We use dataset [11] that Shumon Huque has published in his blog. This dataset has been processed beforehand by Shumon Huque. In this dataset, response size and request size are recorded. However, there is no timestamp. So we made a simulation of a DNS amplification attack, which is explained in detail in the following subsection.

### *B. Pre-processing of experiment data*

Since there is no timestamp in each packet in the original dataset, that is, we have no information about the frequency of attack packets. So we have to simulate the number of requests per unit time by using a random function of C language. In addition, amplification of normal communication is assumed to about 20, expanding multiples of attacks is assumed to about 100. In order to investigate a drawback of this detection method, we think such a situation is reasonable. In Fig.4 and Fig.5, the frequency width is narrow, which means that the intensity of the attack is weak (attack frequency is near to normal frequency). So in this situation, the false positive is happen easily. The result of classification is shown in Fig.4 and Fig.5.

### *C. Results and analysis of experiment*

As shown in Fig.4 and Fig.5, the horizontal axis represents the frequency (frequency of requests in the simulated unit

time), the vertical axis is an enlarged multiple (ratio of response traffic to the request traffic in one unit time).

- In the case of k=2

As shown in Fig.4, the total of points was divided into two (red and blue) clusters. The red one is identified to abnormal and the blue one is identified to normal. However, the far left of the red cluster (18, 109.17) was classified to the abnormal cluster because of its large multiple. Though this point has large multiple, it is should be a normal data since the frequency is so low. And in other case, when the attacker sends to the server that performance is bad as a target, then classification would become more difficult and there is also a possibility that the erroneously detected to the normal data. The reason for this appearance is considered that inadequate numbers of the feature.

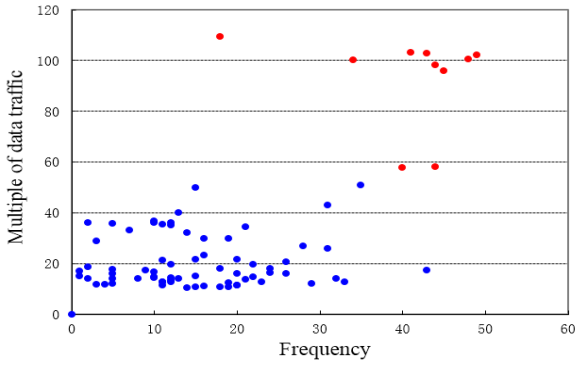


Fig.4 Clustering result when k=2.

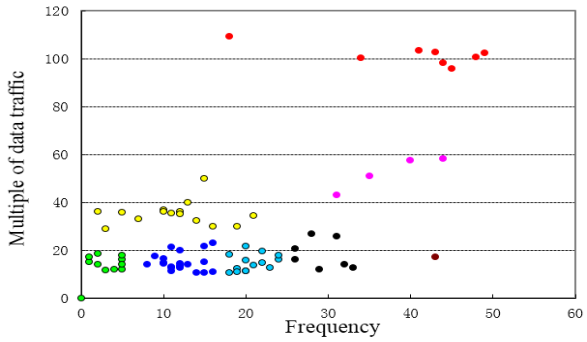


Fig.5 Clustering result when k=8.

- In the case of k=8

Fig.5 is the clustering result when k=8. The data were divided into eight clusters. The red cluster contains DNS amplification attacks. Although pink cluster is almost the same as the normal state, whether it normal or abnormal is determined by server's performance.

Comparing the two situations when k=2 and k=8, we can see that the classification is in more detail. For example, the point (43, 17.14) also can be distinguished from the other data. However, like the case of k=2, point (18, 109.17) is still erroneously classified. That is, even the number of clusters (k) has got up to 8, the classification result has still problems. In order to solve this problem, a new feature will be introduced in our experiment II, which will be explained in the next section.

## VI. Experiment II

In experiment II, besides the two features used in Experiment I, a new feature is added. The new feature is the ratio of the number of the response packets to that of the request packets. And the method for making a detection pattern is like the experiment I, dividing into groups of normal and abnormal by using k-means algorithm, and records reference point of each group. While putting the new data, calculate the distance between data and each reference point to determine which groups it should go. Compared with the experiment I, there is no necessary to cluster new data and considered that the accuracy of detection would be increased in utilizing three features.

### *A. Experiment dataset*

At experiment II, we use Shumon Huque's dataset [11] (same as experiment I) to simulate attack appearance and use kdd cup 99 dataset [12] to simulate normal appearance. In addition, in order to analyze the relationship of attack strength and detection rate, we assumed frequency 1 is normal and use the random function to simulate the attack strength in the 1, 2, 3 … 10, 15 times of normal frequency.

### *B. Results and analysis of experiment*

As shown in Fig.6, the horizontal axis is the intensity of attack (the ratio of the request frequency of attacks to that of the normal), the vertical axis is the percentage of the simulated data being reported as attacks. In this experiment, we assumed the cases with greater than or equal to seven times of normal frequency are DNS amplification attacks with a high probability.

As shown in Fig.6, as the frequency of attack is increased, the value of each feature becomes closer to the reference point of the abnormal group, so it can be seen that the detection rate is increasing. When using the method of research [7] at attack strength 2, 93.39% of total attacks are actually detected. And if two features (blue) are used, the detection rate is 91.27% when the attack strength is 3. Compared with these, it exceeds 95% if three features (pink) are used to detect at attack strength 4. In other words, the method of the existing research [7] and the case of using two features are more sensitive to determine it is abnormal. But there is a possibility that occurs to erroneously detect the normal state to attack in low frequency.

When the attack frequency is the same as the normal frequency (the value of horizontal axis is 1), the detection rate became 19.86% if the two features are used. And the existing research and the method using three features both have detection rate 0% in this case. Such low detection rates are reasonable considering, that the DNS server will receive the same amount of attack requests and normal requests and in

actual amplification attacks, the attack frequency is always much greater than the normal frequency.

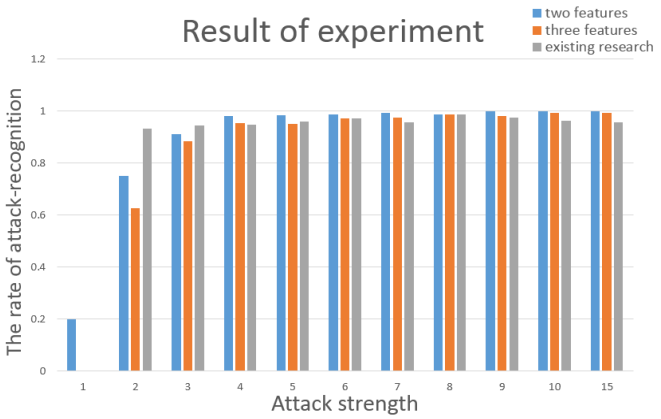


Fig.6 The rate of attack-recognition.

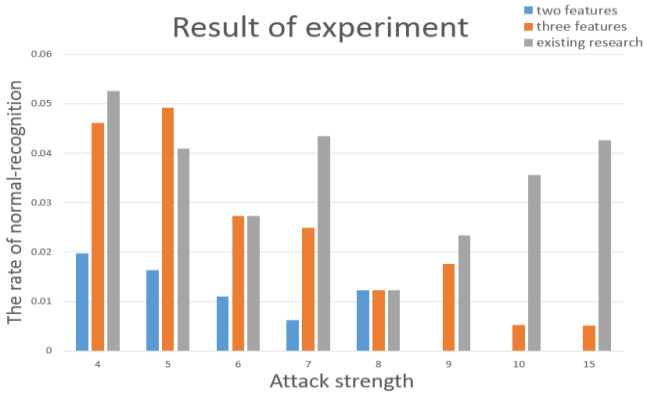


Fig.7 The rate of normal-recognition.

## VII. Related work

Many of methods for detecting and limiting the DNS amplification attacks have been proposed. For example, detection by response rate [13], detection by the table showing the correspondence between request and response [14], a method detecting an abnormal server from the server group by the deviation value [7].

In [13], Paul Vixie and Vernon Schryver introduce a method to limit the DNS amplification attack by recording the response frequency, not the frequency of DNS queries. It will stop the acceptance of the inquiries when the frequency of response exceeds a certain threshold. Because of such operation, the frequency of response will decrease. If this value is below the threshold, DNS server would resume the acceptance again. In other words, this mechanism ensures that the frequency of every query does not exceed the threshold. Therefore, it is possible to realize to reduce the effects of DNS amplification attacks. However, it is necessary to determine the threshold for each DNS server. Whether or not the maximum rate of false positive is able to be cut down is determined by the method of determining the threshold.

In method [14], detection by a table showing the relationship between request and response can possibly find the DNS amplification attacks by analysis the information of inquiry and response. However, because a large amount of corresponding information has to be recorded, this method itself can lead to overload. In some cases, there is a tendency that the efficiency is reduced in reverse.

In paper [7], the number of increased replies and the number of requests by the DNS server are used as a step ladder expressed by the mathematical formula, to determine the state of normal and abnormal by a threshold. From the formula in the paper, we can know that, from the time when the number of replies is three times of the number of requests, it becomes easy for the DNS server to be recognized as abnormal one. However, since the detection method uses the number of requests and the ratio of the number of requests to the replies, even in the cases that there are many requests, no attacks will be reported if the number of the ratio is small.

As shown in Fig.7, when the high frequency of attack occurs, the detection rates of using two features and using three features are both higher than the existing studies [7] (The vertical axis in Fig.7 is the rate of normal-recognition for comparing results of three methods). In the case of 7, the rate of normal-recognition of two features is 0.62%, the rate of three features is 2.48% and the rate of existing researching is 4.35%. In particular, if the attack frequency is greater than or equal to 7 times of the normal frequency, our method has more stability and higher detection rate than the existing research [7]. In the case of 15, the rate of normal-recognition of two features is 0.00%, the rate of three features is 0.51% and the rate of existing researching is 4.26%. This is seeming because that the existing research [7] just utilizes the relation of increased number of packets and number of the request packets.

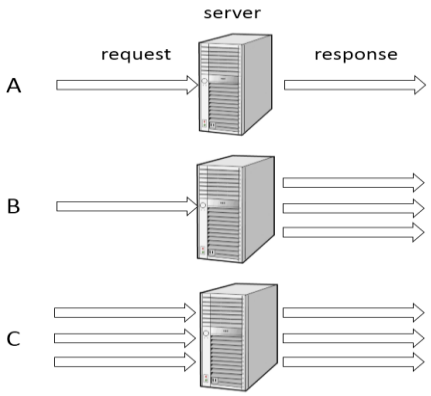


Fig.8 Situation that a request pass through a DNS server.

As shown in Fig.8 C, although it doses not generate a large number of replies, if the number of requests has reached a considerable amount, is also can effectively attack victim's network through the DNS server. In this case, the DNS amplification attacks having small amplification just looks like a DDoS attack, which cannot be effectively found by the existing research [7]. In our study, because the frequency is also used as one of the features, so such kind of attacks can be reported. Further, the reason that, in some cases, the detection rate of using two features is higher than that of using three

features is as follows. Although using the third feature can avoid false positive at low frequency, it leads to relatively low detection rate at high frequency. Even so, we can see its performance is better than the existing research.

## VIII. CONCLUSIONS

In this paper, we proposed a detection method of DNS amplification attacks using three features (frequency of request, multiple of data traffic, the ratio of a number of the reply packets to that of the request packets). We simulated the situation when the DNS amplification attack happened. We extracted the necessary features from simulated traffic and then, using the k-means algorithm to classify the normal cluster and the abnormal cluster to make detection pattern and calculate the reference points. Further, compared and analyzed the results of simulation experiments. The result of the simulation experiment indicates that our proposal is better than existing research [7]. But our research has two challenges, which will be faced in our future work.

The first one is the weight of each feature. In the current study, we assumed that three features have the same importance, but it is necessary to consider whether they have the same impact on the network. Another one is looking for new features which can further improve the detection performance.

## REFERENCES


[1] Damas J, Graff M, Vixie P. Extension mechanisms for DNS (EDNS (0))[J]. 2013.

[2] Alexiou N, Basagiannis S, Katsaros P, et al. Formal analysis of the kaminsky DNS cache-poisoning attack using probabilistic model checking[C]//High-Assurance Systems Engineering (HASE), 2010 IEEE 12th International Symposium on. IEEE, 2010: 94-103.

[3] Friedl S. An Illustrated Guide to the Kaminsky DNS Vulnerability (2008)[J].

[4] Cowperthwaite A, Somayaji A. The futility of DNSSec[C]//Annual Symposium Information Assurance (ASIA). 2010.

[5] Deshpande T, Katsaros P, Basagiannis S, et al. Formal analysis of the DNS bandwidth amplification attack and its countermeasures using probabilistic model checking[C]//High-Assurance Systems Engineering (HASE), 2011 IEEE 13th International Symposium on. IEEE, 2011: 360-367.

[6] Kambourakis G, Moschos T, Geneiatakis D, et al. A fair solution to DNS amplification attacks[C]//Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on. IEEE, 2007: 38-47.

[7] Sun C, Liu B, Shi L. Efficient and low-cost hardware defense against DNS amplification attacks[C]//Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE, 2008: 1-5.

[8] http://www.atmarkit.co.jp/ait/articles/0112/18/news001.html

[9] http://blog.csdn.net/lycb_gz/article/details/11720247

[10] http://e-words.jp/w/DNS_amp.html

[11] http://blog.huque.com/2013/04/dns-amplification-attacks.html

[12] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[13] Vixie P, Schryver V. “DNS response rate limiting(DNSRRL),”ISC-TN-2012-1-Draft1(2012).

[14] GEORGIOS K, TASSOS M, DIMITRIS G, et al. A fair solution to DNS amplification attacks[A]. Proceedings – 2nd International Annual Workshop on Digital Forensics and Incident Analysis[C].2007.38-47