Pak. J. Biotechnol. Vol. 13 special issue II (International Conference on Engineering and Technology Systems (ICET'16) Pp. 35 - 39 (2016)

MITIGATION OF DENIAL OF SERVICE ATTACK USING ICMP BASED IP TRACKBACK

J. Gautam, M. Kasi Nivetha, S. Anitha Sri and P. Madasamy

Department of Information Technology, Velammal College of Engineering and Technology
Madurai, India
gjp@vcet.ac.in, kasinivetha2096@gmail.com, anitha2827@gmail.com, o.samy39@gmail.com

ABSTRACT: Denial of Service (DoS) is a major threat in Network Communication which floods a remote host network with large amount of traffic thereby denying services to the legitimate computer requesting resources. In this paper an ICMP traceback message scheme is proposed to solve the problem of finding the true origin of packets causing DoS. The main objective is to propose a method to trace back the attacker without the involvement of reflector in order to reduce the traffic. The proposed method is a hybrid of bloom filters and iTrace. This method reduces the traffic and the number of ICMP messages. In bloom filters, edge router produces the ICMP messages and in iTrace each router generates ICMP messages.

Index Terms—ICMP, iTrace, Denial of service, reflector attack.

I. INTRODUCTION

A Network is a group of interconnected nodes that are capable of sharing packets between many nodes from source to destination. Wireless technology transmits data packets through a wireless media say radio waves. There are various threats to network thus security to network is much important. Network Security is a way of designing a secured network thereby to prevent it from unauthorized access, misuse, malfunction, destruction, or improper disclosure. The designed networking infrastructure should provide usability, reliability and safety of your network and data. It should prevent threats from entering and spreading into the network thereby enhancing the performance of the network.

ICMP in the network layer is an error reporting protocol and is used by routers, hosts and network devices to generate error messages when there are problems delivering IP packets. ICMP sends error message to the source when error occurs. There are several attacks in network. Of that Denials of service (DoS) attacks have become a major threat to current computer networks since it increases time delay and packet drop and decreases the throughput [8]. DoS attacks consume a remote host or network's resources, thereby denying or degrading service to legitimate users. Typically, adversaries conduct DoS attacks by flooding the target network and its computers with a large amount of traffic from one or more computers under the attacker's control [3]. Such attacks are toughest to address since they are simple to implement, hard to prevent, difficult to trace.

Another attack is reflective DoS attack or reflector attack, in which a legitimate third party component sends traffic to a victim. The attacker imitates the victim's IP address by ultimately hiding its own identity [4]. Then the attackers send packets to the reflector servers and it send ("reflect") back the response to the victim's IP address. Thus, from the servers' perspective, the victim sent the original request. In order to prevent from degradation of service IP traceback is implemented. IP traceback is a process of determining the origin of a packet. Initially a forwarded packet is stored in the edge router where the packet's IP address is stored and then it is forwarded further to the destination.

II. RELATED WORK

MyungKeunYoona [10] proposes a simple generic solution called path addresses to provide new information to the internet which simplify the design of security system. The performance evaluation shows that it reduces overhead and the false positive ratio and the false negative ratio can also be made negligibly smaller.

Arun [6] proposes that detection of distributed denial of service attacks and reflector attacks is performed using an adaptive and hybrid neuro-fuzzy systems. This paper proposes a NFBoot algorithm in which the accuracy of detection is high and few false alarms are generated. The drawback of this paper is that they can only detect and filter the attack traffic but do not perform IPTraceback to catch the attackers.

Hiroshi et al., [12] proposed a method based on request response relationship. It monitors the request response at the edge router. In this method response for the packet is allowed only if the corresponding request is found. The request and reply does not follow the same path in case of routing asymmetry this is the disadvantage of this method.

Al-Duwairi et al., [13] proposed a solution for the routing symmetry that is the reply packet is validated and paired in a distributed manner with the corresponding request packet. The drawback of this paper is that edge routers coordination is difficult and it requires a lot of message exchanges.

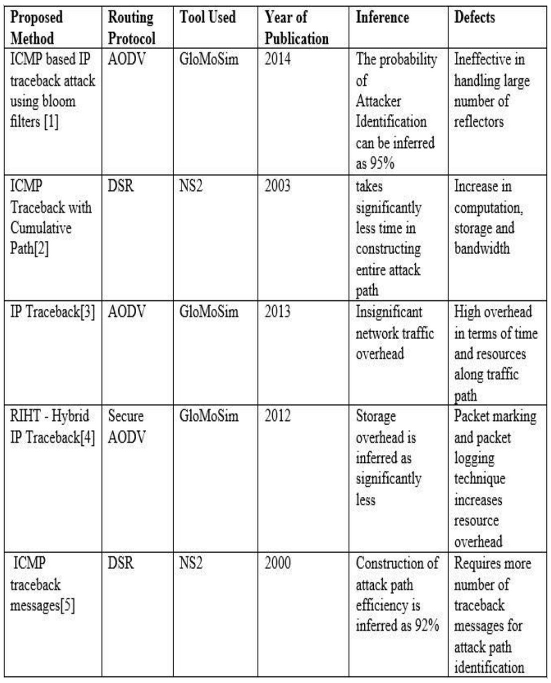
Shui Yu [9] has proposed a traceback method based on entropy variations between normal and DDoS attack traffic is implemented for DDoS attack. This proposed method has various advantages such as its memory is non-intensive, efficiently scalable, robust against packet pollution, and independent of attack traffic patterns.

Yang Xiang [8] proposed two metrics such as generalized entropy metric and information distance metric are used to identify the DDoS attack. These metrics can detect the attack several hops earlier. This paper also suggests that IP Traceback algorithm can detect the attack and attackers and discard the traffic.

HongchengTian and Jun Bi [11] have proposed a Sample Trace, which builds an AS-level overlay network for incremental deployment is suggested. This eliminates the need for using any dedicated trace back software and hardware at routers for deployment.

Barros [5] suggested to let the routers to send ICMP traceback message to the packets destination with enough traceback message from the router it is easy to find the source of the attack which in turn results in increasing the traffic of a routing path. Henry et al., [2] in this paper proposed a ICMP Traceback with Cumulative Path (ITrace-CP) is used to encode the entire attack path information in the ICMP Traceback message. This approach performance provides faster construction of the attack graph but only marginal increase in computation, storage and performance.

Saurabh and Sairam [1] proposes to trace back the path Reverse iTrace method is implemented which identifies the source without the use of reflector. Additive and multiplicative bloom filters are embedded with the reverse iTrace in order to avoid the huge amount of traffic and it also reduces the number of iTrace. Gateway Link Trace paper [7] proposes a method for the mitigation of DoS attack using bloom filters and Reverse itrace, bloom filters used here are Additive and Multiplicative Bloom Filters, which reduces the number of iTrace generated approximately by 100 times.



Proposed Method	Routing Protocol	Tool Used	Year of Publication	Inference	Defects
ICMP based IP traceback attack using bloom filters [1]	AODV	GloMoSim	2014	The probability of Attacker Identification can be inferred as 95%	Ineffective in handling large number of reflectors
ICMP Traceback with Cumulative Path[2]	DSR	NS2	2003	takes significantly less time in constructing entire attack path	Increase in computation, storage and bandwidth
IP Traceback[3]	AODV	GloMoSim	2013	Insignificant network traffic overhead	High overhead in terms of time and resources along traffic path
RIHT - Hybrid IP Traceback[4]	Secure AODV	GloMoSim	2012	Storage overhead is inferred as significantly less	Packet marking and packet logging technique increases resource overhead
ICMP traceback messages[5]	DSR	NS2	2000	Construction of attack path efficiency is inferred as 92%	Requires more number of traceback messages for attack path identification

Fig. 1. Inference of related works

III. ICMP TRACEBACK

For dealing with Denial of Service attacks where the source IP is forged and for the detection of asymmetric routers the path of the packet in the internet is important. There are methods such as traceroute which provide the forward path but not reverse. To fix this issue an ICMP Traceback message is used. While forwarding packets, routers can generate traceback message to send along with packets to the destination. The source where traffic generated and path travelled can be determined only if there are sufficient traceback messages from enough routers along the path. It is reported [1,14] that the routers in the path generate ICMP messages or iTrace with very small probability. The packet and router information is contained in the iTrace packets. All routers in the path will get enough chance to send iTrace packets to the victim during flooding based DoS attacks. By this the victim can traceback the attacker.

IV. PROPOSED WORK

The main objective is to propose a method to traceback the attacker without the involvement of reflector in order to reduce the traffic. The proposed method is a hybrid of bloom filters and iTrace. This method reduces the traffic and the number of ICMP messages. In bloom filters, edge router produces the ICMP messages and in iTrace each router generates ICMP messages.

A. Simulation-Network Formation

Simulation is regulated using NS2 2.35. Because of the link stability and route lifetime, no route overhead was considered in our simulation. In 500 X 500 area, mobile nodes exist. Square area is used to increase average hop length of a route with relatively small nodes. Every mobile node is moving based on the mobility data files that were generated by mobility generator module. A number of 50 nodes are created. The transmission range is fixed at 100 meters. 100 nodes have destinations and try finding routes to their destination nodes. Maximum speed of node is set to 20 m/sec. The nodes are assigned with an initial position. All nodes do not stop moving and the simulation time is 500 seconds

ICMP traceback is the method of back tracking the path. IP packet passes from slave to the victim through the router. This router generates the ICMP messages for every 20000 packets. ICMP messages are otherwise known as iTrace messages. This iTrace messages consists of the router id and the information about the packet which caused its generation.

This iTrace message generated by the router is sent to the victim. During flooding based DoS attack, each router in the path will generate the message and sent it to the victim. By this the victim can traceback the attacker.

TABLE I. Simulation Parameters

Parameter	Value
Coverage area	500mx500m
Simulation Time	500s
No of nodes	50
Traffic Type	UDP-CBR
Packet Size	512 bytes
Maximum Speed	20 m/s
Routing Protocol	AODV
Mobility Model	Random Way Point

Reverse iTrace is the method in which the iTrace messages are sent to the slave instead of the victim. The router will send the messages to the slave if the slave deceives the request message from victim. At this point the slave will act as the victim and through this the victim can traceback the path without the involvement of reflector. During DoS attack the source will receive the message from all the routers in the path through which the packets are sent.

Bloom filter method reduces the traffic overhead and also maintains the traceback success rate. To reduce the number of traceback messages, the source attack has to be found directly instead of tracing the attack path. This is done by two bloom filters such as Additive Bloom Filters (ABF) and Multiplicative Bloom Filters (MBF). Additive bloom filters block the messages generated by legitimate traffic and Multiplicative bloom filters bounds the number of traceback messages. The addition of these two filters helps to generate the messages at the start of the attack as soon as possible

The proposed method is a combination of itrace and the bloom filter method which is capable to traceback the attacker with less trace overhead. In iTrace each router has to generate ICMP messages periodically for every 20000 packets while in bloom filter method only edge router is generating ICMP messages for long source flows and sends to the victim.

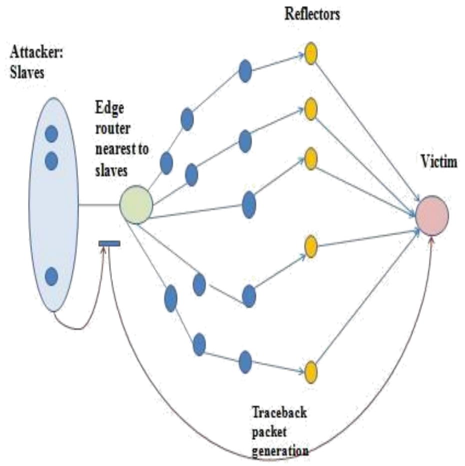
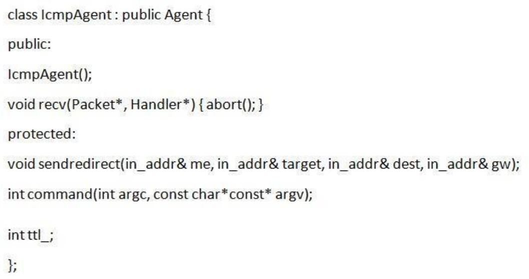


Fig. 2. Reflector attack trace backing method

Fig 2 shows the pictorial representation of the proposed method. The main part of the system is the edge router that will generate the ICMP messages consists of edge router id to the victim for every 20000 packets. The victim receives and processes the packets and identifies the edge router id from which the packet sent and traces back to the attacker.



```
class IcmpAgent : public Agent {
public:
IcmpAgent();
void recv(Packet*, Handler*) { abort(); }
protected:
void sendredirect(in_addr& me, in_addr& target, in_addr& dest, in_addr& gw);
int command(int argc, const char*const* argv);

int ttl_;
};
```

Fig. 3. ICMP Packet generation

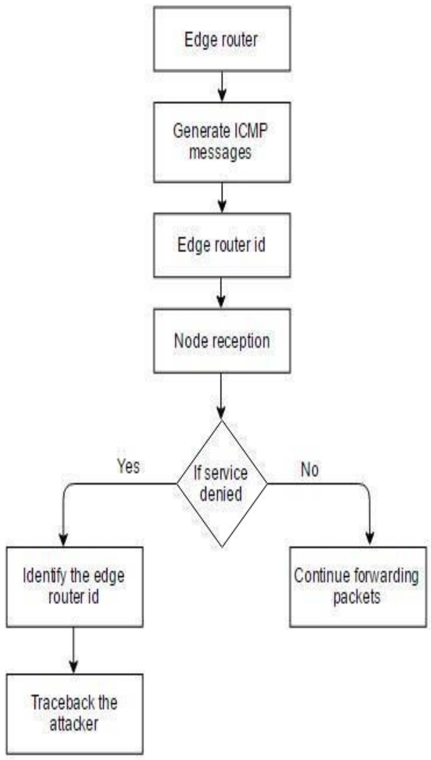


Fig. 4. Depicting the behaviour of victim nodes

B. Itrace Generation

Itrace is generated by the routers that have minimum hop count from the source i.e., closer to the source. In a packet switched network, full path IP traceback is as good as finding the address of the edge router nearest to the attacker in terms of identifying the attacker.

In a given network, all attack packets from the slaves pass through this edge router before fanning out into numerous paths as can be seen in Fig 2. This common starting point of attack generates enough number of iTrace packets to allow traceback to be performed at the victim. If the victim receives iTrace message from this router, it can identify the attacker.

Hence, in our proposed traceback model, only the edge router nearest to the source of packet is allowed to generate iTrace message. This strategy has two major advantages. First, it saves iTrace generation by all other routers in the path and hence reduces number of ICMP messages generated.

Assuming the average Internet path length to be 15, such a scheme will cause 15 times less overhead trace. The second advantage is that, it makes traceback independent of the number of reflectors involved in the attack. Because, no matter how much the paths diverge, they all diverge from this router.

Hence, if the victim receives iTrace message from this router, it can identify the attacker. This makes our method much more scalable and helps in handling highly distributed and large scale reflector attacks

V. EXPERIMENT ANALYSIS

Table II shows that as simulation time increases the variation in the number of ICMP packets generated for both the proposed method and the bloom method is shown. At the end of simulation, the ICMP packets generated by proposed method is 6 whereas bloom method generates 72 ICMP packets. This reveals that the proposed method reduces traffic by generating less ICMP packets than other existing methods.

For the values given in Table II a graph is plotted and it is shown in Fig 5. The graph clearly shows that the number of ICMP messages generated for the proposed method for a given simulation time is less than that of the ICMP messages generated for the bloom filter method at that particular time.

TABLE II. ICMP packets generated

Simulation Time (Seconds)	ICMP Packets Generated	
	Proposed Method	Bloom Method
50	1	12
100	2	24
150	3	36
200	4	48
250	5	60
300	6	72

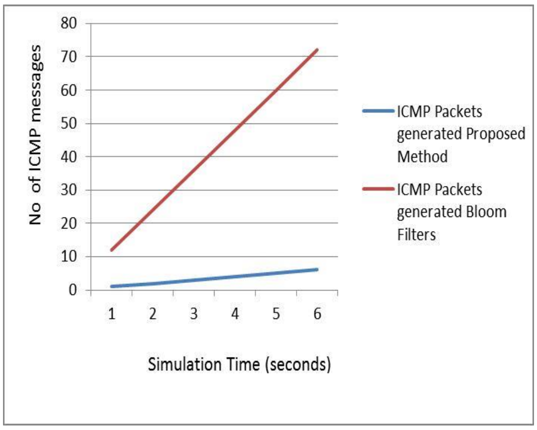


Fig. 5. Comparison of ICMP packet generation

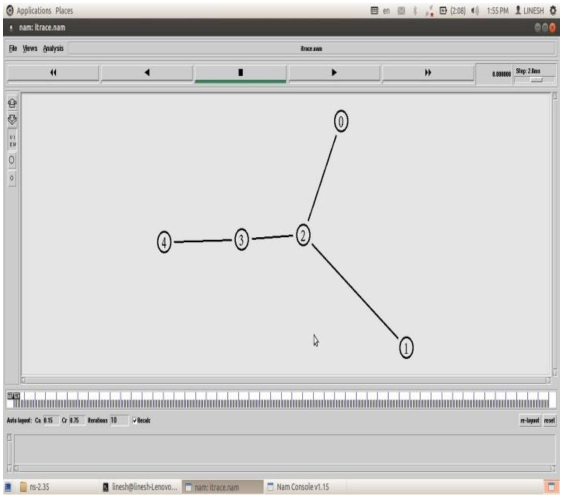


Fig. 6. Topology generated using NS2-2.3

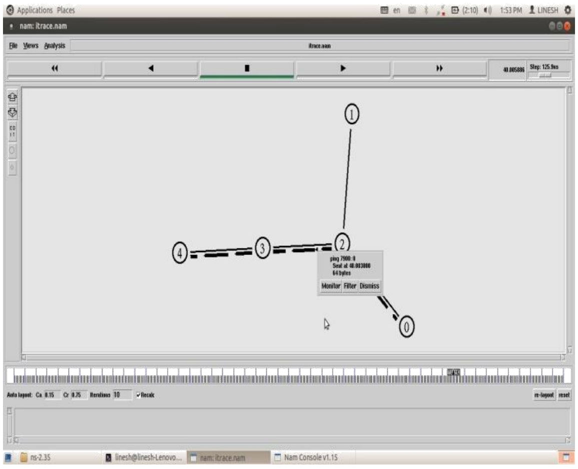
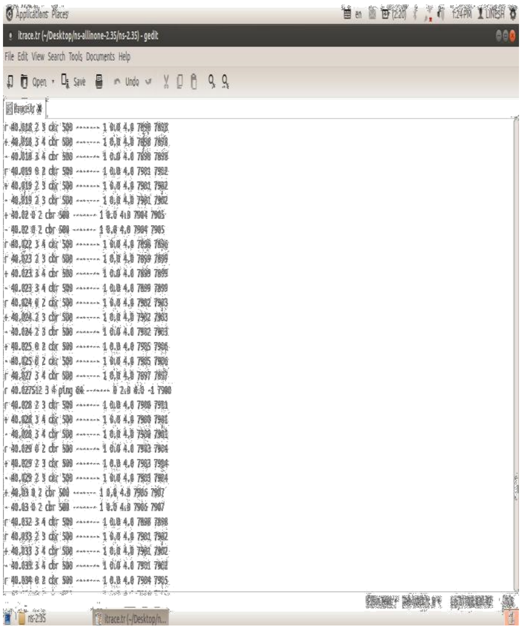


Fig. 7. Generation of ICMP


Applications Places
itrace.tr (~/Desktop/ns-allinone-2.35/ns-2.35) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
itrace.tr
ns-2.35
itrace.tr (~/Desktop/n...

```
r 40.018 2 3 cbr 500 ------- 1 0.0 4.0 7898 7898
+ 40.018 3 4 cbr 500 ------- 1 0.0 4.0 7898 7898
- 40.018 3 4 cbr 500 ------- 1 0.0 4.0 7898 7898
r 40.019 0 2 cbr 500 ------- 1 0.0 4.0 7901 7902
+ 40.019 2 3 cbr 500 ------- 1 0.0 4.0 7901 7902
- 40.019 2 3 cbr 500 ------- 1 0.0 4.0 7901 7902
+ 40.02 0 2 cbr 500 ------- 1 0.0 4.0 7904 7905
- 40.02 0 2 cbr 500 ------- 1 0.0 4.0 7904 7905
r 40.022 3 4 cbr 500 ------- 1 0.0 4.0 7896 7896
r 40.023 2 3 cbr 500 ------- 1 0.0 4.0 7899 7899
+ 40.023 3 4 cbr 500 ------- 1 0.0 4.0 7899 7899
- 40.023 3 4 cbr 500 ------- 1 0.0 4.0 7899 7899
r 40.024 0 2 cbr 500 ------- 1 0.0 4.0 7902 7903
+ 40.024 2 3 cbr 500 ------- 1 0.0 4.0 7902 7903
- 40.024 2 3 cbr 500 ------- 1 0.0 4.0 7902 7903
+ 40.025 0 2 cbr 500 ------- 1 0.0 4.0 7905 7906
- 40.025 0 2 cbr 500 ------- 1 0.0 4.0 7905 7906
r 40.027 3 4 cbr 500 ------- 1 0.0 4.0 7897 7897
r 40.027512 3 4 ping 64 ------- 0 2.0 4.0 -1 7900
r 40.028 2 3 cbr 500 ------- 1 0.0 4.0 7900 7901
+ 40.028 3 4 cbr 500 ------- 1 0.0 4.0 7900 7901
- 40.028 3 4 cbr 500 ------- 1 0.0 4.0 7900 7901
r 40.029 0 2 cbr 500 ------- 1 0.0 4.0 7903 7904
+ 40.029 2 3 cbr 500 ------- 1 0.0 4.0 7903 7904
- 40.029 2 3 cbr 500 ------- 1 0.0 4.0 7903 7904
+ 40.03 0 2 cbr 500 ------- 1 0.0 4.0 7906 7907
- 40.03 0 2 cbr 500 ------- 1 0.0 4.0 7906 7907
r 40.032 3 4 cbr 500 ------- 1 0.0 4.0 7898 7898
r 40.033 2 3 cbr 500 ------- 1 0.0 4.0 7901 7902
+ 40.033 3 4 cbr 500 ------- 1 0.0 4.0 7901 7902
- 40.033 3 4 cbr 500 ------- 1 0.0 4.0 7901 7902
r 40.034 0 2 cbr 500 ------- 1 0.0 4.0 7904 7905
```

Fig. 8. Trace file of packet generation

VI. CONCLUSION AND FUTURE WORK

The method proposed will traceback the attacker in the reflector attack environment. Using this method traceback is done without the involvement of the reflectors. The proposed method reduces the number of ICMP messages generated and as a result produces an optimum traffic overhead in the network. By the mathematical analysis, it is found that the number of ICMP messages generated is optimum. In future, the small and large flows are identified and differentiated and hence the false negative rate will be reduced.

REFERENCES

[1] S. Saurabh and A.S. Sairam, ICMP based IP traceback with negligible overhead for highly distributed reflector attack using bloom filters, Computer Communications 42: 60-69 (2014).

[2] Henrym C.J. Lee, Vrizlynn L.L. Thing, YiXu and Miao Ma, ICMP Traceback with Cumulative Path, An Efficient Solution for IP Traceback,

[3] IP Traceback: A New Denial-of-Service Deterrent? IEEE Security and privacy, 1540-7993, IEEE (2013).

[4] Ming-Hour Yang and Ming-Chien Yang, RIHT: A Novel Hybrid IP Traceback Scheme, IEEE Transactions on Information Forensics and Security 7(2): April (2012).

[5] Barros, A proposal for ICMP traceback messages (2000). from:http://www.research.att.com/lists/ietfitrace/2000/09/msg00044.html.

[6] P. Arun, Raj Kumar, S. Selvakumar, Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems, Computer Communications (2012).

[7] Gateway Link Trace, umass Network Trace Repository, (2005). http://traces.cs.umass.edu/index.php/Network/Network.

[8] Yang Xiang, Ke Li, and Wanlei Zhou, Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, IEEE Transactions on Information Forensics and Security 6(2): June (2011).

[9] Shui Yu, Member, Wanlei Zhou, Robin Doss, and WeijiaJia, Traceback of DDoS Attacks Using Entropy Variations, IEEE Transactions on Parallel and Distributed Systems 22(3): March (2011).

[10] MyungKeunYoona, An incrementally deployable path address scheme, ShigangChenb, Elsevier, Journal of Parallel Distributed Computing 72: (2012).

[11] HongchengTian and Jun Bi, An Incrementally Deployable Flow-Based Scheme for IP Traceback, IEEE Communication letters 16(7): July (2012).

[12] T. Hiroshi, K. Ohta, A. Yamamoto, N. Ansari, Y. Waizumi, Y. Nemoto, Detecting DRDoS attacks by a simple response packet confirmation mechanism. Comput. Commun. 31(14): 3299–3306 (2008).

[13] Basheer Al-Duwairi and G. Manimaran, Distributed packet pairing for reflector based DoS attack mitigation. Comput. Commun. 29: 2269–2280 (2006).

[14] Izaddoost Alireza, Mohamed Othman and Mohd Fadlee A. Rasid, Accurate ICMP traceback model under DoS/DDoS attack. International Conference on Advanced Computing and Communications, ADCOM-07, IEEE, (2007)