International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 01, January 2017
www.ijates.com
ijates
ISSN 2348 - 7550

DISTRIBUTED DENIAL OF SERVICE ATTACKS IDENTIFYING USING FORD FULKERSON ALGORITHM IN CLOUD

R. Devi[1] , R. Shanmugalakshmi[2]

[1]*Information Technology, Government College of Technology, Coimbatore, Tamilnadu, India.*

[2]*EEE, Government College of Engineering, Salem, Tamilnadu, India.*

ABSTRACT

Nowadays many service providers are available all throughout the world. This service provider provides different types of services. Customers or organizations that need for service will register with service providers and get services through Internet. Since the services are provided through Internet, services may be blocked to legitimate customers due to DDoS (Distributed Denial of Services). Ford Fulkerson algorithm is used to identify the DDoS attack. This algorithm is used to identify the maximum flow of the unidirectional network.

Keywords: DDoS attack, Ford Fulkerson, network flow, service providers.

I. INTRODUCTION

This paper specifies the importance of identifying DDoS attack in the Internet through which the legitimate users utilize the services provided by the service provider.

Service providers can be an organization which develop services and deploy them in the cloud. Legitimate user can be a person or organization which utilizes the services provided by the service providers through Internet.

DDoS – [1] Distributed Denial of Service is an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resource. UDP flood attack and ping of death attack are the two attacks that are considered for this paper.

Ford Fulkerson algorithm is used to determine the maximum flow of an unidirectional network. [2] As long as there is a path from the source (start node) to the sink (end node), with available capacity on all edges in the path, we send flow along one of these paths. Then we find another path, and so on. A path with available capacity is called an augmenting path.

Once the maximum flow augmenting path is determined the flow gets forwarded in that direction. Similarly in this algorithm service provider is assigned to source and legitimate user is assigned to sink. Capacity of the network link is assigned to bandwidth between the nodes. Intermediate nodes are the routers between the source and sink. Three or four major frequently used paths are selected and they are plotted as a network.

Ford Fulkerson algorithm determines maximum flow between the source and sink, the augmenting path is unidirectional from source to sink. But in the case of Internet all are bidirectional; that is the destination can request for service and the source provides service as reply. Split the bidirectional network into two

unidirectional networks. Instead of max flow capacity calculation, [4] max flow bandwidth is calculated between the source to sink. This max flow bandwidth is taken as the threshold to identify DDoS attack. The first two sections of this paper deals with Ford Fulkerson algorithm for network flow and bandwidth calculation and the next two section specifies the attacks of DDoS and how to identify that DDoS attack using Ford Fulkerson algorithm.

II. FORD FULKERSON ALGORITHM

[12] Let G (V, E) be a graph where V represents number of vertices in the graph and E represents number of edges in the graph. Let C (u,v) be the capacity of the edge between the node u and v. Let f(u,v) be the flow between the node u and v. Then the following equations are formulated,

Capacity

$$: \forall (u,v) \in E \; f(u,v) \leq C(u,v) \qquad (1)$$

Skew symmetry

$$: \forall (u,v) \in E \; f(u,v) = -f(v,u) \qquad (2)$$

By applying the above initial conditions eq.1 and eq.2 the following algorithm determines the max flow in the network.

Algorithm:

a. Input: graph G with flow capacity C of each edge, a source node s and a sink node t.
b. Output: max flow of the network from s to t.
c. Assign flow $f(u,v) \leftarrow 0$ for all edges (u,v)
d. Identify the path between s and t using Breath First Search or Depth First Search
e. While there is a path P from s to t in G_f, such that $C_f(u,v) > 0$ for all edges $(u,v) \in P$
   i. Find $C_f(P) = \min \{C_f(u,v) : (u,v) \in P\}$
   ii. For each edge $(u,v) \in P$

$$f(u,v) \leftarrow f(u,v) + C_f(P)$$

$$f(v,u) \leftarrow f(v,u) - C_f(P)$$

f. Finish

Algorithm 1

For example, consider the following graph with six vertices

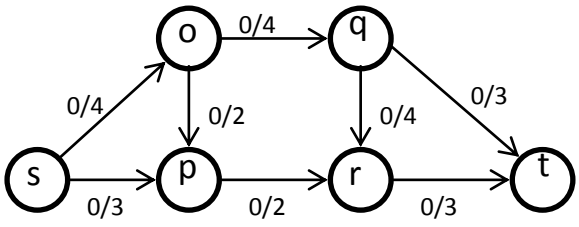


Figure 1

s- Source t- Sink

0/4 – flow/capacity o,p,q,r – intermediate nodes

Augmenting path 1 (s,o,q,t) flow = min{4,4,3} = 3

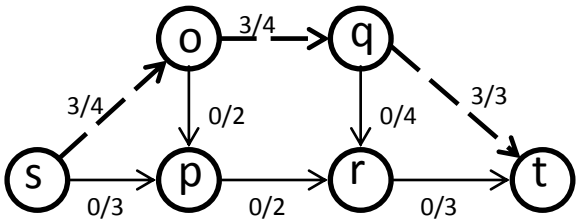


Figure 2

Augmenting path 2 (s,p,r,t) flow = min{3,2,3} = 2

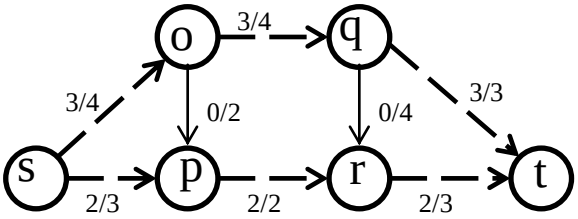


Figure 3

Augmenting path 3(s,o,q,r,t) flow = min{1,1,4,1} = 1

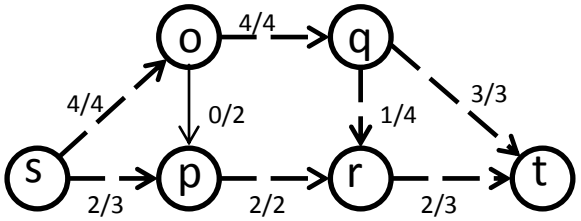


Figure 4

Max flow = sum {Augmenting path1+Augmenting path2+Augmenting path3}

=3+2+1 = 6

Hence, Max flow of the given graph is 6.

III. FORD FULKERSON ALGORITHM FOR NETWORK BANDWIDTH CALCULATION BETWEEN SERVICE PROVIDER AND LEGITIMATE USER

Consider most frequently used three different paths as graph G (V, E) where V represents number of interconnecting devices in the graph and E represents number of edges between the interconnecting devices in the graph. Frequently used paths can be calculated using trace back option of the packet which traverses from source to destination.

The flow of Internet [2] is bidirectional, but Ford Fulkerson algorithm will work on directed graph. If the graph is acyclic then the non-terminating problem of Ford Fulkerson algorithm will not occur [2]. Hence the identified bidirectional network between the service provider and legitimate user should be represented as two separate acyclic graphs. But here only the direction from the service provider to the legitimate user is taken into account.

This is because the service provider will have enough security services like firewalls, updated antivirus patching, etc., the legitimate users are not aware of all security services where ever they utilize the services.

Let B(u,v) be the bandwidth [3] of the edge between the node u and v. Let f(u,v) be the flow between the node u and v. Then the following equations are formulated,

Capacity

$$:\forall(u,v) \in E\ f(u,v) \leq B(u,v) \quad (3)$$

Skew symmetry

$$:\forall(u,v) \in E\ f(u,v) = -f(v,u) \quad (4)$$

Consider the same figure Fig.1 as a bidirectional graph.

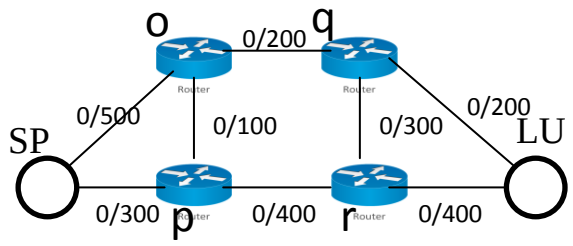


Figure 5

SP – Service Provider; LU – Legitimate User;

o,p,q,r – Routers; 0/500 – flow/bandwidth(Mb/s)

Fig.5 is represented as two different directed acyclic graphs as follows.

Direction from SP to LU:

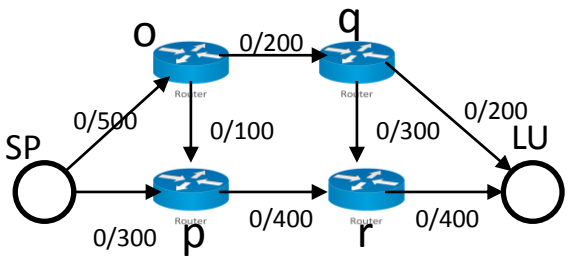


Figure 6

Direction from LU to SP:

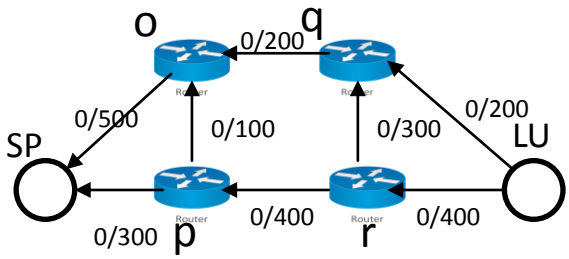


Figure 7

In this paper Fig.6 is considered. By applying the above initial conditions in equations (3) and (4) the following algorithm determines the optimized bandwidth [4] in the network. By applying the algorithm 1 the following augmenting paths are generated.

Augmenting path 1 (SP,o,q,LU)

Flow = min {500,200,200} = 200

Augmenting path 2 (SP,p,r,LU)

Flow = min {300,400,300} = 300

Augmenting path 3 (SP,o,p,r,LU)

Flow = min {300,100,100,100} = 100

Optimized bandwidth = sum {Augmenting path1+Augmenting path2+Augmenting path3} (5)

=200+300+100 = 600

Hence optimized/maximum bandwidth between SP and LU is 600 Mb/s

IV. DDOS ATTACKS IN INTERNET

Distributed Denial of Services attack consists of components such as attacker who controls the slaves (zombies) which in turn flood the packets to the victims system [1] by avoiding the services to the legitimate users. [5] Some of DDoS attacks in network layer are i) flooding attacks like bandwidth flooding attacks, protocol exploitation flooding attacks, reflection based flooding attacks, amplification based flooding attacks and some of DDoS attacks in application layer are ii)HTTP flooding attacks, session flooding attacks, slow request attacks, slow reading attacks.

Bandwidth flooding attacks and amplification based flooding attacks are the two attacks that can be identified using Ford Fulkerson algorithm. Existing mitigation methods for the prevention of DDoS are [5] SOS (Secure Overlay Services), WebSOS (uses SOS architecture and graphic turing test), Fosel (filtering by helping an overlay security layer), CLAD (Cloud Based Attack Defence system), [13] IDS (Intrusion Detection systems), CISCO IOS Netflow, etc.

Already existing victim side defences [13] for DDoS attack is to use hop count filtering method using TTL (Time To Live) field in IP packets. TTL is verified with an initial value and the original hops value the packet traversed in the network. If the difference between the initial value hop count and the original value hop count is positive then there is no DDoS attack, if it is negative then the victim system is compromised to DDoS attack. [6] Other defencing method is EDoS-Shield and its key components are virtual firewalls (VF) and a cloud-based verifier node (V-Nodes).

V. DDOS ATTACK IDENTIFICATION ALGORITHM USING FORD FULKERSON METHOD

The above said DDoS prevention methods are wrapped around web servers that belong to the service provider side. This paper specifies a method using Ford Fulkerson algorithm for calculating [4] optimized bandwidth between the service provider and legitimate user. After calculating the optimized bandwidth if there is any

DDoS attacks in legitimate user side that can be identified using the following algorithm 5.1. The importance of victim side defence is, the legitimate user may unaware of security measures to safeguard their systems, they may not patch their antivirus software, etc.

Algorithm for optimized bandwidth:

a. Input: graph G with network bandwidth B of each edge, a source node SP (Service Provider) and a sink node LU (Legitimate User).
b. Output: Optimized bandwidth of the network from SP to LU.
c. Identify most commonly used 3 paths from SP to LU using single packet Trace back method [7].
d. Assign flow $f(u,v) \leftarrow 0$ for all edges (u,v)
e. Identify the path between SP and LU using Breath First Search or Depth First Search
f. While there is a path P from SP to LU in G_f, such that $B_f(u,v) > 0$ for all edges $(u,v) \in P$
a. Find $B_f(P) = \min \{B_f(u,v) : (u,v) \in P\}$
b. For each edge $(u,v) \in P$

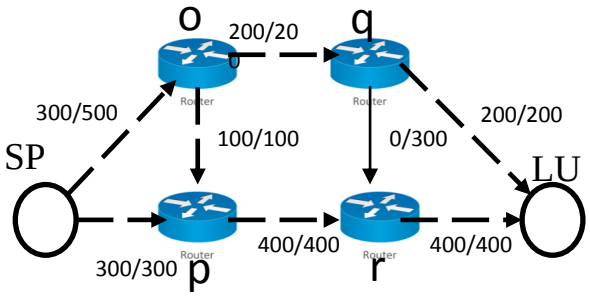
$$f(u,v) \leftarrow f(u,v) + B_f(P)$$

$$f(v,u) \leftarrow f(v,u) - B_f(P)$$

g. Call algorithm DDoS attack identification
h. Finish

Algorithm 2

If the above algorithm 2 is applied for the Fig.6 then the optimized bandwidth network calculation using Ford Fulkerson algorithm is shown below.



Max bandwidth = 600mb/s

Figure 8

Here the maximum bandwidth is 600 Mb/s as calculated in III chapter. Using this optimized bandwidth calculation algorithm the proposed algorithm for DDoS attack identification is given below.

Algorithm for DDoS attack identification:

a. Input: output of algorithm 5.1 with optimized network bandwidth from a source node SP (Service Provider) to the sink node LU (Legitimate User).
b. Output: return **true** if there is **no DDoS attack** else return **false** if there is **DDoS attack**.
c. If the legitimate user not able to request or receive services from service providers then
    i. Calculate the available bandwidth (AB) between the SP and LU

$$AB = \sum_1^n A(P) \qquad \text{eq.5}$$

Where n= number of paths between

SP and LU, A (P) augmenting

max flow in path P

ii. If AB > OB (Optimized bandwidth calculated using algorithm 5.1) then

Return false

iii. Else

Return true

d. Else

Print the legitimate user is able to receive the service from the service provider.

Return true

e. Finish

Algorithm 3

The algorithm 3 is explained with an example as shown below

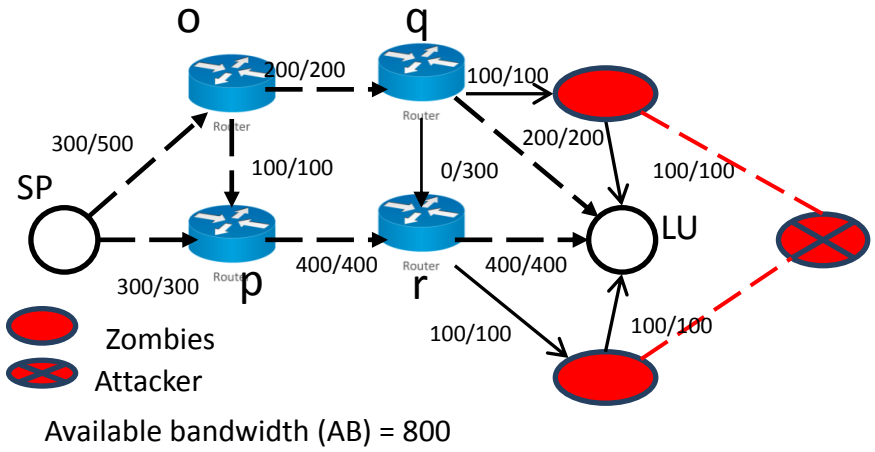


Figure 9

According to Fig.9, the attacker creates zombies as slaves and start flooding LU [8]. Hence the available bandwidth calculated as 800 Mb/s which is greater than optimized bandwidth 600Mb/s calculated from Fig.9 Hence the algorithm return false identifying that LU is affected by DDoS attack.

VI. RESULTS AND ENHANCEMENTS

Ford Fulkerson algorithm helps in the identification of DDoS attack in the Internet. By considering the optimized bandwidth as a reference the available bandwidth is calculated during random period of time and its result is shown below.

Table 1

	R(t1)	R(t2)	R(t3)	R(t4)	R(t5)	R(t6)
Optimized bandwidth	600	600	600	600	600	600
Available bandwidth at time R(tx)	300	400	200	500	800	500

In Table 1, the available bandwidth is calculated at random time value x using the proposed algorithm and the optimized bandwidth is calculated using Ford Fulkerson algorithm. The optimized bandwidth is taken as reference bandwidth. During random period of time the available bandwidth is calculated and compared with the optimized bandwidth.

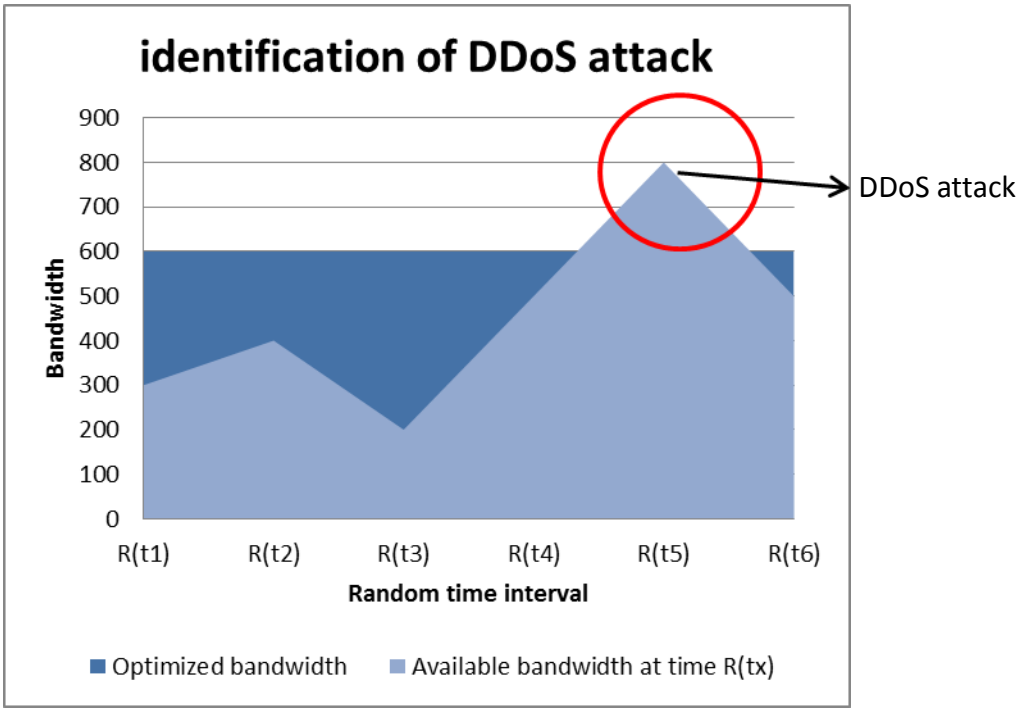


Figure 10

From Fig.10, during random time R(t5) AB> OB and it is identified that the occurrence of DDoS attack

The following points are some of the enhancement features,

- Just the detection of DDoS attack is not enough; it should include how to avoid it?
- Quantitative threat assessment of DoS attack [9] can be included to increase the service availability of services.
- Identification concept should be wrapped around frame work / network architecture to enhance its security.
- Paths are selected statically which are incompatible with the real time networks. They should be selected dynamically.
- User can access the service from any place in the world but the algorithm based on static location

VII. CONCLUSION

This paper proposes a method for optimized bandwidth calculation as well as DDoS attack detection with optimized bandwidth as reference. [14] Capacity planning is necessary for the e-business environment; this algorithm helps for this capacity planning. [10] To calculate the maximum response time an algorithm is needed to identify the maximum flow between the source and destination. [11] Cloud zombie is one of the proposed algorithms for detecting DDoS attack in cloud environment. [16] Netflow analyzer is a tool which is used to analyse and plan the capacity of the network for network administrator.

By considering all this information this algorithm is simple and efficient for calculating optimized bandwidth as well as the detection of DDoS attack in cloud environment.

REFERENCES

Journal Papers:

[1] Abhishek Jain, Ashwani kumar Singh "Distributed Denial of Service (DDoS) Attacks - Classification And Implications" published by Journal of Information and Operations Management, Volume 3, Issue 1, pp-136– 140, 2012

[2] Wojcik, R., Domzal, J., Dulinski, Z. , "Flow-Aware MultiTopology Adaptive Routing". Communications Letters, IEEE , vol.18, no.9, pp.1539,1542, Sept. 2014

[3] Dwivedi, A., Xinghuo Yu , "A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis". Industrial Informatics, IEEE Transactions, vol.9, no.1,pp.81,88, Feb. 2013

[4] Eclides pinto neto, Gustavo callou , "An approach based on Ford Fulkerson Algorithm to optimize network bandwidth usage" IEEE (Brazilian symposium on computing systems engineering), 2015.

[5] Wael Alosaimi, Mazin Alshamrani, Khalid Al-Begain, "simulation based study of DDoS of service attacks prevention in the cloud" IEEE (9th International conference on Next Generation Mobile app, services and technologies), 2015.

[6] Wael Alosaimi, Mazin Alshamrani, Khalid Al-Begain, "Denial of Service Attacks Mitigation in the Cloud" IEEE (9th International conference on Next Generation Mobile app, services and technologies), 2015.

[7] Ning Lu, Yulong Wang, Fangchun Yang, Maotong Xu, "A Novel Approach for Single-Packet IP Traceback Based on Routing Path" IEEE (20th Euromicro International Conference on Parallel, Distributed and Network-based Processing), 2012.

[8] C.Kavitha, "Complete Study on Distributed Denial of Service Attacks in the Presence of Clock drift" IEEE (ICICES2014) 2014.

[9] Xiuzhen Chen, Shenghong Li , Jin Ma "Quantitative Threat Assessment of Denial of Service Attacks on Service Availability", IEEE, 2011

[10] Nihat Altiparmak and Ali Saman Tosun "Integrated Maximum Flow Algorithm for Optimal Response Time Retrieval of Replicated Data" CPS(41st International Conference on Parallel Processing), 2012

[11] Saeed, ShafieianMohammad, ZulkernineAnwar Haque, "CloudZombie: Launching and Detecting Slow-Read Distributed Denial of Service Attacks from the Cloud" IEEE International Conference on Computer

and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.

Books:

[12] ”Design and analysis of algorithm” book by Cormen.

[13] Qijun Gu, Peng Liu, “Denial of Service attacks” Pennsylvania state University.

[14] IBM Global Services, “ Network performance and capacity planning: Techniques for an e-business world”