IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Securing internet by eliminating DDOS attacks

To cite this article: R Niranchana *et al* 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042099

View the article online for updates and enhancements.

Securing internet by eliminating DDOS attacks

R Niranchana, N Gayathri Devi, H Santhi and P Gayathri
School of Computer Science and Engineering, VIT University, Vellore -632014, India

E-mail: hsanthi@vit.ac.in

Abstract. The major threat caused to the authorised usage of Internet is Distributed Denial of Service attack. The mechanisms used to prevent the DDoS attacks are said to overcome the attack's ability in spoofing the IP packets source addresses. By utilising Internet Protocol spoofing, the attackers cause a consequential load over the networks destination for policing attack packets. To overcome the IP Spoofing level on the Internet, We propose an Inter domain Packet Filter (IPF) architecture. The proposed scheme is not based on global routing information. The packets with reliable source addresses are not rejected, the IPF frame work works in such a manner. The spoofing capability of attackers is confined by IPF, and also the filter identifies the source of an attack packet by minimal number of candidate network.

1. Introduction

Serious Threat to the Internet is Distributed Denial of service attacks [23], [24], [25]. More frequently the occurrence of DDoS attacks [6], [14], [19], [24] are seen on an everyday basis in at most all the network backbone whereas IP Spoofing is a major threat that worsens the mechanism in order to policing these attacks. It is caused by the forged source address in the IP packets. An attacker does not reveal his identity and location, by pretending as a different host. The most popular is IP spoofing [1], [2], [5] for the upcoming causes, initially this IP Spoofing [7], [15] is the reason for the legitimate Traffic to become harder by separating the attack traffic, as a result the source address which is spoofed will be available in all over the Internet.

Next, the insertion of the level of indirection can be made easier for the attacker, where as a result more effort is needed to localize the attack traffic source. At last several attacks utilise IP Spoofing [16] and acquires the strength and becomes more able in order to forge source addresses. The original path which routes the packet to the destination cannot be controlled, even the attackers may insert a source addresses which is termed to be arbitrary inside the IP packets.

Depending on the above conclusion route base packet filters was been suggested to present the IP spoofing [8]. The Assumption here is, single path routing, only one path P(s,d) is from source s to the destination node d. Thus, a packet with source address s and destination address d, which is found in a router, and not present in P(s,d) is to be dropped. The construction of the packet filer based on the route information is a huge challenge. By using Global routing information, where it is much complicated to accommodate in the current routing infrastructure for Internet [13], [17], [22].

As there are several Autonomous System (AS) all over the Internet [9]. On utilizing the Border Gateway Protocol (BGP) every AS [11] and its nearby neighbour communicate with each other. BGP is termed to be a policy-based routing protocol that formulates certain policies for routing [3] in which selection as well as propagation of the best route to the destination at the ASs, is been guided using routing policies [20] defined locally. The Route-base Packet filter [10] construction is considered as the biggest challenge in the present Internet [8], [12] regime of routing.

Here an Inter domain Packet Filter(IPF) is proposed, which is constructed depending on the BGP Updates, with the assumption where every ASs utilize an routing policies [21] which is in usage currently.

2. Literature Survey

Ref. No	Title	Inferences
[1]	Internet Protocol Spoofing in VOIP	The various spoofing types, detection and prevention of spoofing attacks are studied
[2]	IP spoofing and its Detection Technique	DPM (deterministic packet marking) and PPM (probabilistic packet marking) in networking is been proposed
[3]	Privacy-Preserving Interdomain Routing at Internet Scale	MPC approach for interdomain routing is been discussed
[4]	Quantifying AS Path Inflation by Routing Policies	The AS path inflation on the end-to-end path from end users to two popular content providers, Google and Comcast is investigated
[5]	Secure Verification Technique for Defending IP Spoofing Attacks	An (SVT) for defending IP spoofing attacks is been proposed
[6]	Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing	Here low-rate TCP-targeted DoS attacks can have severe impact on the Border Gateway Protocol (BGP) is studied
[7]	Controlling IPSpoofing Through Packet Filtering	Route-based Packet Faltering (PF) of incoming data packets is proposed
[8]	Modeling DDoS Attacks with IP Spoofing and Hop-Count Defense Measure Using OPNET Modeler	The methodology for modeling a DDoS UDP flood with an IP spoofing attack and hop count defense is focused here.
[9]	Initial longitudinal analysis of IP source spoofing capability on the Internet	The capability of IP Spoofing on the Internet studied.
[10]	On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets	Evaluate route-based distributed packet filtering (DPF), a novel approach to distributed DoS (DDoS) attack prevention.
[11]	Modelling Autonomous–System Relationships	A novel algorithm for generating synthetic graphs, annotated with AS relationships, that reproduce these AS relationships-aware properties has been proposed.

[12]	Consensus Routing: The Internet as a Distributed System	A single mechanism that can address all of these consistency problems in policy routing is Designed.
[13]	Interconnection, Peering and Settlements	In this paper they have examined both the technical and business aspects which surround this ISP interaction, commonly referred to as "interconnection, peering and settlements"
[14]	A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks	The scope of the DDoS flooding attack problem and attempts to combat it is studied.
[15]	Spoofing Prevention Method	The new approach for filtering spoofed IP packets, called Spoofing Prevention Method (SPM), is proposed.
[16]	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing is been proposed.
[17]	BGP4: Inter-Domain Routing in the Internet	BGP4: Inter-Domain Routing in the Internet is studied.
[18]	Limiting Path Exploration in BGP	They have proposed a simple, novel mechanism forward edge sequence number to annotate the AS paths with path dependency information. Then EPIC, an enhanced path vector protocol is described.
[19]	Detection Architecture of Application Layer DDoS Attack for Internet	This paper designs two independent architectures for HTTP and FTP which uses an extended hidden semi-Markov model is proposed.
[20]	Internet Routing Policies and Round-Trip-Times	In this paper, They have explored some of the ways in which routing policies impact RTTs and how routing policies for both intra- and inter-domain routing is been investigated.
[21]	A Survey of Inter domain Routing Policies	The survey of results shed light on routing policies used in practice and on the extent to which common modeling assumptions about routing policies actually hold on the Internet is done.

[22]	Why Is It Taking So Long to Secure Internet Routing?	This article has concentrated on protocol-based attacks on BGP.
[23]	TDPF: a Trace back-based distributed packet filter to mitigate spoofed DDoS attacks	They have proposed a trace back-based distributed packet filter (TDPF), and a novel distributed packet filtering mechanism that employs IP trace back as a means for traffic discrimination.
[24]	Denial-of-service attack-detection techniques	Denial-of-service attack-detection techniques are studied.
[25]	Survey on DDoS Attacks and its Detection & Defence Approaches	In this paper, a review on the current DoS and DDoS detection and defence mechanism studied.

3. Proposed System

3.1 Interconnections of Border Gateway Protocol and AS

Internet's AS graph (Figure. 1) is depicted as Undirected graph G = (V, E), where every node q ε V denotes an AS, then every edge E(*u, q*) ε F denotes an BGP session in between the nearby ASs *u, q* ε V. The assumption made here is, there is only one edge in between a pair of neighbouring ASs. Every node has one or a number of network prefixes. The BGP [13] route updates are exchanged by nodes, where they are made as either announcements or withdrawals in order to know the alternations about reachability through the destination network prefixes. Usually a list of route attributes related with destination network prefix present in the route announcements. Among the attributes, the path vector attributes AS_path, where it is the path vector of ASs [4] through which the route is propagated, next Local_pref attribute, denotes the local preference degree which is related with each route. Then R.as_path , R.Local_pref and R.prefix is needed to represent the as_path, the Local_pref, and the destination network prefix of 'R'. Then if R.as_path = $\{q_k\, q_{k-1} \ldots . q_1 q_0\}$. From node q_0 the route is to be originated, where q_0 has the network prefix r.prefix. The route is traversed through the nodes $q_1,q_2,..q_{k-1}$ prior arriving at the node q_k, in the same order. Where I = k, k-1..1, then the edge $E(q_i,q_{i-1})$ is found on the path of AS, where $E(q_1,q_{i-1})$ ε R.as_path. Table.1 shows the notations used.

Table 1. Notations used in AS

Notations Used	Descriptions
BGP	Border Gateway Protocol
DDoS	Distributed Denial of Service
AS	Autonomous System
E,V	Edge, Vertex
S, D	Source, Destination
R	Route

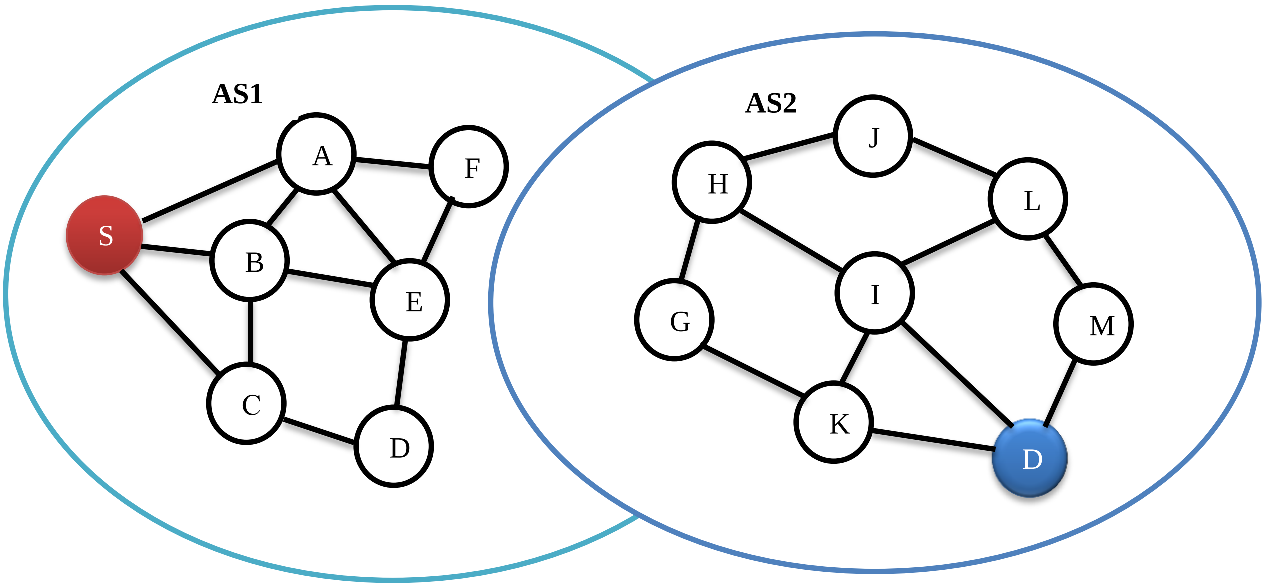

Figure 1. Sample Autonomous Networks

Clearly, the route node R, along with its AS path R.as_path are used, then a specific destination AS *d* is also taken into consideration where the route announcements, withdrawals are to be more specific towards the network prefix, which is owned by the node *d*, ‘*d*’ also denotes the network prefixes which is owned by ASs *d*. Then the route R which is utilised to attain the network prefix owned by ‘*d*’ destination will be denoted as the route to *reach destination* ‘*d*.

3.1.1 Policies, along with Route selection

Every node chooses, and propagates to neighbours a single *best* route to reach destination. Routing policies which are locally defined, governs the choosing and propagation of *best* routes. An individual node chooses and propagates to the nearby nodes, as an optimized rate to destination. Routing policies [23] formulated locally, are in-charge of policies followed. The pair of policies for routing are usually made in use by a node are Import and Export policies. Import policies are made in use by the routes which are learned from the nearby nodes, Export policies are used on the basis of locally choosen *best* route, in prior to their propagation into the nearby node.

“Desirability of the routes is affected by the import polices, by changing the attributes of the route, Hence ‘*t*’ is the route (towards the destination *d*) obtained at *q* from node *v*, altered route which is been changed by import policies is represented as import(*q*←*v*)[{*t*}}. The altered route is updated in the Database routing table of ‘*q*’. Then **candidateZ**(q, d) is the notation of the set of routes altogether:

$$\textbf{candidateZ}(q,\, d) = \{t : import(q \leftarrow v)[\{t\}\} \neq \{\}$$
$$t.prefix = d,\ \forall v\ \ \varepsilon\ \ N(q)\ \}.$$

Where, N(q) is the set containing neighbours of ‘q’.

Candidate routes Z(q, d), node q chooses the *best* route for reaching the Destination on the basis of an early formulated procedure. The output of the procedure of selection at the node *q*, is marked as the *best* Route as *best*Z(q, d) from *candidate*Z(q, d), *q* usually is in charge to export the route to the nearby node on making use of export polices which are neighbour specific. These policies decide if the route is sent to near by node, if yes they alter the parameters of the route on the basis of policies *export*(*q* →*v*) [{*t*}] is the route which is forwarded to nearby node *v* by node *q*, after node *q* uses the export policies on the route *t*.

In response to the events of the network the updates as obtained, hence BGP is an incremental protocol. If any event does not occur, updates about the route is not triggered or exchanged among the neighbours. The routing system is considered to be in a stable state.

Stable routing state: A routing system is considered to be in a stable state when every node has choosen the optimal route to reach other nodes and route updates are not generated.

3.1.2 AS Relationships, Routing Policy

The AS uses certain routing policies [4], [20] internally which is defined by economics:
Certain relations are followed by the connection between AS. The below said arrangements is to be entered by a pair of AS.

- **Provider to customer**- Here the provider AS is paid by the customer AS to take over its traffic, which is more usual if the provider, is larger when compared to the customer in size.
- **Peer to peer**- By a mutual peering agreement AS. Choose to carry all the traffic from each other. They are not supposed to carry transit traffic by each other.
- **Sibling to sibling** – Here mutual transit service is provided by the two Ass.

The Ass and neighbour relationship is determined by export and import policies which are neighbour specific. Rules of policies are followed are in the Table 2[25], 3[21] and [23]. These are the rules which is used by Ass on the Internet currently.

Table 2, where r_1 and r_2 specifies the routes to *d*, which is obtained by node q by the neighbour's v_1 an v_2. *Customer*(*q*), *peer*(*q*), *provider*(*q*), *sibling*(*q*) represents the customer set, peers, providers then the siblings of node *u*. From Table 2, as will be choosing the routes mentioned in that. In Table 3 r_1-r_4 denotes export policies utilised by Ass to specifically to announce routes to providers, customer, peers, and siblings.

Table 2.
Import Routing policies at an AS

if ((v_1 є *customer* (u) ∪ *sibling*(u))
and (v_2 є *peer*(u) ∪ *provider*(u))) then
r_1.local_pref > r_2. local_pref

Table 3.
Export Routing Policies at an AS

Export rules		**r1**	**r2**	**r3**	**r4**
Export routes to		provider	Customer	peer	sibling
learned from	provider	no	yes	no	yes
	customer	yes	yes	yes	yes
	peer	no	yes	no	yes
	sibling	yes	yes	yes	yes
Own routes		yes	yes	yes	yes

4. Design of Inter Domain Packet Filters

Using the BGP [18] route information the IPF architecture defines the formulation of IPF and then the validity of IPF's are established. Consider N(*s*, *d*) refers to a packet belonging to the source *s* and destination is *d*. The method for packet filtering, chooses if a packet is to be sent forward or else discarded on the basis of certain issues.

Packet filtering based on Route**:** The packet N(*s*, *d*) is accepted by Node *q* which is sent by the node *v*, if suppose E(*u, q*) є *best*Z(*s, d),* or else the packet's source address is spoofed and also the packet is rejected by *q*.

A packet filter rejects the spoofed packets, and permits the authorized packets to attain the destination, to prevent IP spoofing. Through the packet filter based on route is unable to find the packet spoofed even if it has the perfect information regarding routing, a packet filter which is valid, which does not concentrate on not dropping any authorized packets, which contributes to the ability of reducing spoofed packets. Based on this, the correctness of the packet filter is explained below:

*Packet filtering-correctness***:** If the packet filter is not able to discard packets containing a source address which is valid, that packet filtering is termed as correct, Then the routing system is considered to be stable.

It is clear that, Route-based packet filter is exactly correct, as the packets which is valid, from source *s* to the destination *d* will be traverse through the edges on bestR(*s, d*). Hence in order to calculate the route-based packet filter needs the understanding of bestR(*s, d*) on each and every node, where as it is not possible in BGP. Whereas IPF avoids this issue.

4.1 IPF Overview

A *Topological route* from nodes '*s*' and '*d*' is termed as a path without loop in between two nodes. A Topological route is termed as feasible route within BGP if route construction do not follow the routing policies [25] formulated by the AS's relationship (as in Table).
*feasible*Z(*s, d*) represent the routes which are feasible from s and d.
*feasible*Z(*s,d*) is explained as below

$$\mathit{feasible}Z(s,d) = \{[s \oplus U \quad \mathit{feasible}Z(v, d)]\}$$

v:
import $(s \leftarrow v)[\{ t \}] \neq \{ \}$,
t.prefix $= d,\ v \in$ N(s)

For example, if {*s ⊕ {[ab],[uv]}*} = {[*sab*], [*suv*]}. The *feasible*Z(*s, d*) has the routes in between the pair and also they do not offend the routing policy-import and export as in Table 2 and Table 3, then *best*Z(*s, d*) ϵ *candidate*Z(*s, d*) ⊆ *feasible*Z(*s, d*). Every feasible route is considered to be a candidate route from the BGP routing table.

Assume a possible route *t* ϵ possible Z(*s, d*). An edge(*v, q*) is on a possible route where E(*v, q*) ϵ *t* as path, then node *v* is called as the possible upstream neighbour of node *q* of the packet N(*s, d*). A set of all the possible upstream neighbours of *q* is represented as possible T(*s, d, q*).

The perception at the base of the framework of IPF is given below: By utilising the BGP route updates, a node *q* is able to find its possible upstream neighbours. The method for learning possible upstream neighbour is explained in the section below: subsequently *best*Z(*s, d*) ϵ *candidate*Z(s, d) ⊆ possible Z(*s, d*) only N(*s, d*) is permitted by the node among the possible upstream to pass by and reject the alternate packets. Hence filtering doesn't reject packets with legitimate source addresses.

Next as a Huge number of topological routes is denoted by network connectivity from source to destination, the profitable relationship from AS and policies of routing used by AS, tends to limit the size of possibleZ(*s, d*). From the example in the Figure 2, Figure 3 (a), Figure 3 (b) shows the topological routes indicated by the routing policies from source *s* to destination *d*.

In Figure 3 (b), Assumptions made are nodes *e, f, g* has an mutual peering relationship, where *e, f* are providers to *s*. Even the number of Topological routes from source *s* and destination *d* is 10, the routing policy supports only 2 possible routes. The network topology shows, the neighbour node which is able to forward packet, between source to a node, possible routes suggested by routing policy, reduces the set of neighbour. Eg: where the node *d* is considered. The node *e* and *f* are the possible routes from *s* to *d*, where node d show that the number of forwarded packets by node *g* from source *s*, has an spoofed address so it is to be rejected. Hence IPF is not much efficient than route based packet filter, because IPF, because IPF are calculated depending on *feasible*Z(*s, d*) not on *best*Z(*s, d*) where, *feasible*T(*s, d, q*) is learnt from the local BGP updates but *best*V(*s, d, q*) does not.

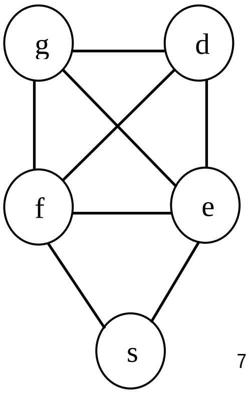

Figure. 2 An example of network Topology

s→e→d
s→f→d
s→e→f→d
s→e→g→d
s→f→e→d
s→f→g→d
s→e→f→g→d
s→e→g→f→d
s→f→e→g→d
s→f→g→e→d

- - - - - - - - Peering relationship

⟶ Provider-customer relationship

S→e→d
S→f→d

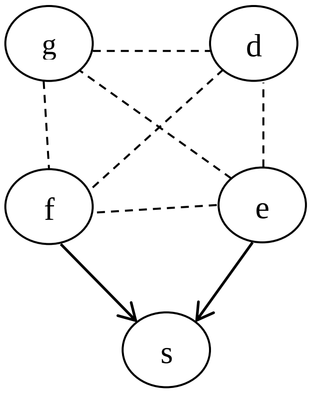

Figure. 3 (b)

Figure. 3 Routes between source **s** and destination **d**. (a) Topological routes implied by connectivity. (b) Feasible routes constrained by routing policies.

4.2 IPF Construction

The theorem below briefs the method for recognizing the possible upstream neighbours of node *q*, for the packet N(*s, d*):

Theorem: suppose a possible route *t* in between source *s* and destination *d* then *q* ϵ *t*.as_path, then set *v* is the possible upstream neighbour of node *q* through *t*. If the routing system is stable, **export**(*u*→*q*)[{***best*R**(*v, s*)}] ≠{}. On the assumption where all the AS adhere to the import and export routing policies in Tables 2 & 3 and every ASs agrees on legitimate routes exported by neighbours. Above theorem denotes, as if node *v* is an possible upstream neighbour of q for packet M(*s, d*), node v has exported to node *q* as its best route to reach source '*s*'.

Proof: Above theorem is applied for all the possible route, which can be of the six types of path. Below the assumption node is, all the possible route *t* is of 6 types where, uphill path is followed in a peer to peer edge, then it is followed by a downhill path. To prove the above theorem the various positions of nodes *v* and *q* in the possible route:

Case 1: Node *v* and *q* belongs to uphill path where node *s* is an sibling of node *v*. The routing policies is Table 2 & the export routing policy r1, then the meaning of indirect customer/siblings, where *v* is propagating to (provider) node *q*, where it is the reachability information of *s*.

Case 2: E(*v, q*) is considered as peer-to-peer end, it can be proved similar to Case 1.

Case 3: The node *v* and *q* is said to be belonging to downhill path, where E(*x, y*) is the peer to peer edge from the possible route '*t*' and note *v* is a customer of *y*. As in the proof of case 2, the node y learns that the reachability information of s from *x*. Using the export routing policy **r2**, the briefing of customers who are indirect, node *y* will propagate through the *s* to node *v*, where the reachability information of *s* to node *q* is further export.

From the above theorem's proof, the possible upstream neighbour for the packet N(*s, d*) can be identified by a node and also it conducts IPF as given below.

IPF Definition: The node *q* will be accepting be accepting the packet M(*s, d*) which is sent by a neighbour node *v*, if export($u \rightarrow v$)[{*best*Z(*v, s*)}] ≠ { }. Or else the packet will be containing spoofed addresses, which in turn causes the packet to be discarded by node *q*.

4.3Creation of Dynamic Routing

Based on the term of assumption AS graph is an static in nature, but the graph changes and triggers the updates on BGP and changing the channels, which AS's makes use of communicate each other, Here the dynamics of routing alters the working of IPF is examined here. Two kinds of routing dynamics are considered a) caused by network failures b) caused because of creating a new network.

When there is a failure of network, the pair of upstream neighbours do not admit other members in the routing convergence period, on the assumption that AS relationships are to be static. If there is a network failure on the routing dynamics type, the function of filters, are not able to block a packet which is valid.

The illustration as below said, Assume an AS *q*, which is said to be IPF enabled is between the Route s to d. then v=*best*T(*s, d, q*) and T=*feasible*T(*s, d, q*). The failure of link or an router within v and s has the following possible outcomes.

a) For AS *v* to reach ASs, *v* is selected as the best upstream neighbour for the packet N(*s, d*) that is *v*=*best*T(*s, d, q*). Here even many routers are explored and broadcasted to *q,* the filtering function of *q* observed, is not affected, while in the process of exploring the path.

b) The AS *v* is not to be considered as the best upstream neighbour for M(*s, d*) packet, and from selecting the another upstream neighbour *v'* ϵ to *v* can be reaching AS *s*. The *v* and *v'* explore multiple routes, as *v'* is been broadcasted as the route to *q*, then IPF belonging to *q* filter the packet M(*s, d*), which is forwarded by *v'*.

c) Then *s* is not at all reachable by upstream neighbours, where AS *q* is unable to reach *s*, hence *q* is not considered as the *best* Route between *s* and *q*. New packet M(*s, d*) cannot be forwarded through *q*.

An Inter Domain Packet Filtering Network model [3] is proposed, where an packet filtering system depending on a router is formed using the values of BGP which is exchanged locally, where the Autonomous System (AS) are having a Routing Policies which are in use from the AS we infer that the formulated global routing information prohibits Flooding when only a manageable few AS's are taken into consideration.

Initially the method to formulate a IPF's at an Autonomous System which makes use of the entries in the BGP exchanges next the guidelines to be followed on which the IPF framework functions in an reliable manner, in the condition where the packets from an legitimate source address is not discarded. At last, the efficiency of the above said architecture is analysed, and an simulation studies on the basics of AS topologies, AS paths are also obtained from the original BGP date. The Analysis shows, the model can actively reduce the spoofing of packets by the Oscar. Suppose if the spoofing of packets are not prevented, IPF is responsible for localization of the Intruder, make belonging to a less number of participants, AS's in turn which can improves the IP trace back situation.

5. Conclusion

An IDF architecture has proposed as an effective countermeasure to the IP Spoofing-based DDoS attacks. IPFs rely on BGP update messages exchanged on the Internet to infer the validity of source address of a packet forwarded by a neighbour. We showed that IPFs can easily be deployed on the current BGP-based Internet routing architecture. The IDPF framework can correctly work without discarding any valid packets. Moreover, they also help pin point the true origin of an attack packet to be within a small number of candidate networks.

References

[1] Jayamali, N N, Munasinghe M G C M, Ariyawansha I C, Kumarathilake Y A, Gunathilaka W S N, Perera R D G and Dhammearatchi D (2016) Internet Protocol Spoofing in VOIP *Imperial Journal of Interdisciplinary Research* **2**

[2] Lavanya M and Sahoo P K (2016) IP spoofing and its Detection Technique *IJACTA* **4** 167-169

[3] Asharov G, Demmler D, Schapira M, Schneider T, Segev G, Shenker S and Zohner M (2017) Privacy-Preserving Interdomain Routing at Internet Scale *Proceedings on Privacy Enhancing Technologies* **3** 1-21

[4] Gao Q, Wang F and Gao L (2016) Quantifying AS Path Inflation by Routing Policies *International Journal of Future Generation Communication and Networking* **9**

[5] Rengarajan A, Sugumar R and Jayakumar C (2016) Secure verification technique for defending IP spoofing attacks *Int. Arab J. Inf. Technol.,* **13** 302-309

[6] Zhang Y, Mao Z M and Wang J (2007) Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing *In NDSS*

[7] Sahu M, Lal R C and Bhilai C (2012) Controlling IP Spoofing Through Packet Filtering *International Journal of Computer Technology and Applications* **3**

[8] Akhter S, Myers J, Bowen C, Ferzetti S, Belko P and Hnatyshin V (2013) Modeling DDoS Attacks with IP Spoofing and Hop-Count Defense Measure Using OPNET Modeler *In Proc. of International Conference OPNETWORK*

[9] Beverly R, Koga R and Claffy K C (2013) Initial longitudinal analysis of IP source spoofing Capability on the Internet

[10] Park K and Lee H (2001) On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets In ACM SIGCOMM *computer communication review* **31** 15-26 ACM

[11] Dimitropoulos X and Riley G (2006) Modeling autonomous-system relationships In Proceedings of the 20th Workshop on Principles of Advanced and Distributed Simulation *IEEE Computer Society* 143-149

[12] John J P, Katz-Bassett E, Krishnamurthy A, Anderson T and Venkataramani (2008) Consensus routing: The Internet as a distributed system. *In Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation* 351-364

[13] Huston G (1999) Interconnection, peering, and settlements. *In proc. INET* **9**

[14] Zargar S T, Joshi J and Tipper D (2013) A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials* **15** 2046-2069

[15] Bremler-Barr A and Levy H (2005) Spoofing prevention method *In INFOCOM 2005 24th Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings IEEE* **1** 536-547

[16] Senie D and Ferguson P (1998) Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing Network

[17] Cheswick W R, Bellovin S M and Rubin A D (2003) Firewalls and Internet security: repelling the wily hacker *Addison-Wesley Longman Publishing Co., Inc.*

[18] Chandrashekar J, Duan Z, Zhang Z L and Krasky J (2005) Limiting path exploration in BGP *In INFOCOM 2005 24th Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings IEEE* **4** 2337-2348

[19] Ankali S B and Ashoka D V (2011) Detection architecture of application layer DDoS attack for internet *International Journal of Advanced Networking and Applications* **3** 984

[20] Zheng H, Lua E K, Pias M and Griffin T G (2005) Internet routing policies and round-trip-times In International Workshop on Passive and Active Network Measurement *Springer Berlin Heidelberg* 236-250

[21] Gill P, Schapira M and Goldberg S (2013) A survey of interdomain routing policies *ACM*

SIGCOMM Computer Communication Review **44** 28-34

[22] Goldberg S (2014) Why is it taking so long to secure internet routing? *Communications of the ACM* **57** 56-63

[23] Fallah M S and Kahani N (2014) TDPF: a traceback- based distributed packet filter to mitigate spoofed DDoS attacks *Security and Communication Networks* **7** 245-264

[24] Carl G, Kesidis G, Brooks R R and Rai S (2006) Denial-of-service attack-detection Techniques *IEEE Internet computing* **10** 82-89

[25] Bhandari N H (2013) Survey on DDoS attacks and its detection & defence approaches *Int. J.Sci. Mod. Eng. (IJISME)* **1** 2319-6386