Controlling IP Spoofing through Inter domain Packet Filters.

Project Guide: Mr. T .Peer Meera Labbai M.tech,(Ph.D).

Project Members:

N.Karthik Kumar (Reg no: 10306083)

Abstract:

- The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet.
- In this project, we propose an Inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet
- A key feature of our scheme is that it does not require global routing information.
- IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers.
- We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses
- In addition, they can help localize the origin of an attack packet to a small number of candidate networks

Objective:

We propose an Inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses.

Existing System:

- Route-based distributed packet filtering (DPF) uses routing information to determine if a packet arriving at a router .
- Border router at an AS—is valid with respect to its inscribed source/destination addresses, given the reach ability constraints imposed by routing and network topology.
- A single AS can only exert a limited impact with respect to identifying and discarding forged IPflows

- As with routing, route-based packet filtering occurs at two time scales—packet forwarding/discard based on table look-up (fast) and filter table update
- Its forwarding/discard function can be performed close to line speed subject to generic processing overhead.

Disadvantages:

- IP spoofing may easily occur. Because the packet-filtering router permits or denies a network connection based on the source and destination addresses of the packet, any attack that uses valid IP address may not be detected.
- Packet-filtering rules are comparatively harder to be designed and configured .

Proposed system:

- A routing system is in a Stable state if all the nodes have selected a best route to reach other nodes and no route updates are generated
- Node v accepts packet M(s,d) that is forwarded from node u if and only if E(u,v) belongs to R(s,d). Otherwise, the source address of the packet is spoofed, and the packet is discarded by v.
- A packet filter is correct if it does not discard packets with valid source addresses when the routing system is stable.

Advantages:

- IDPFs can significantly limit the spoofing capability of an attacker.
- Moreover, they also help pinpoint the true origin of an attack packet to be within a small number of candidate networks, thus simplifying the reactive IP trace back process

Project schedule:

We propose an application called Inter Domain Packet Filter which uses the BGP protocol to check for the genuine packets and discard the spoofed packets . The proposed system uses two basic mechanisms to accomplish the goal:

- Using BGP in routers
- Developing Inter Domain Packet Filter

Phase	Task	Description
Phase 1	Analysis	Analyze the information given in the IEEE paper.
Phase 2	Literature survey	Collect raw data and elaborate on literature surveys.
Phase 3	Design	Assign the module and design the process flow control.
Phase 4	Implementation	Implement the code for all the modules and integrate all the modules.
Phase 5	Testing	Test the code and overall process weather the process works properly.
Phase 6	Documentation	Prepare the document for this project with conclusion and future enhancement.

Module's:

1. Topology Construction
2. BGP Construction
3. IDPF Construction
4. Control the Spoofed Packets

Module 1:

- **Introduction**:

  Topology Construction:

  - In this module we construct a topology structure for our project. Here we tell how the nodes are connected to the other nodes.
  - This will be achieved by socket communication in java.

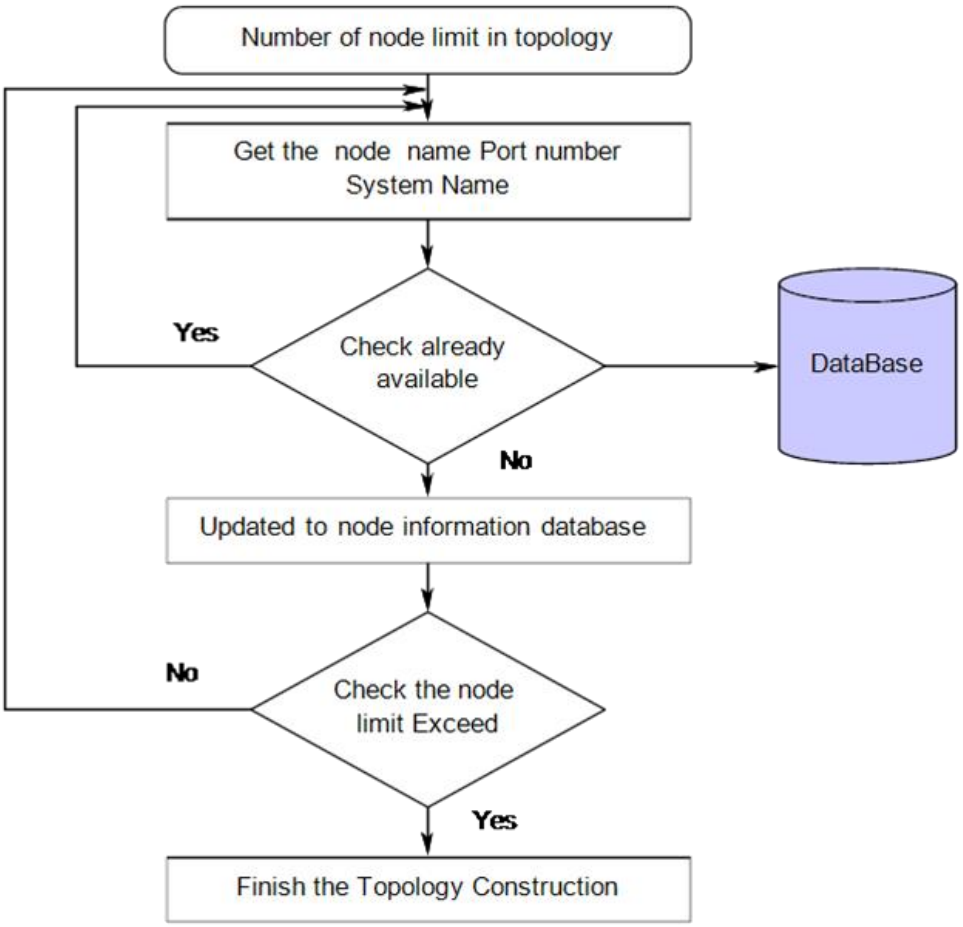
- **Inputs:**

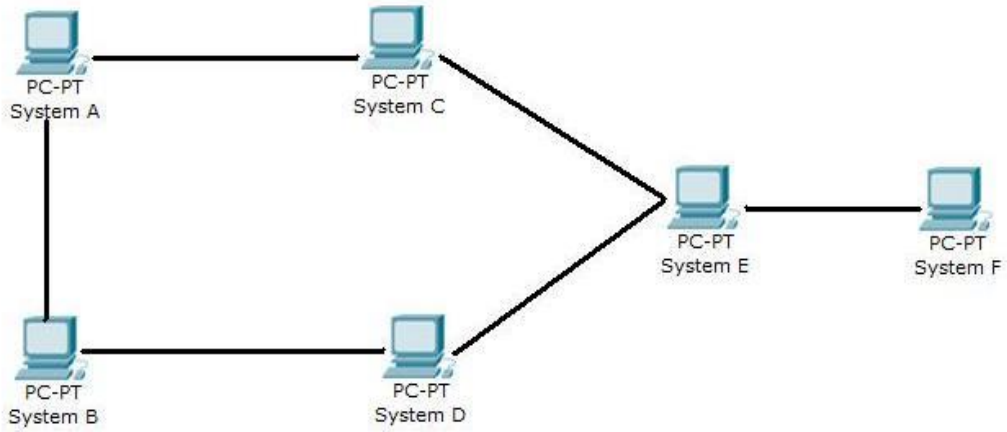
  - Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user.
    - While getting each of the nodes, their associated port and ip address is also obtained.

- **Processing:**

  - For successive nodes, the node to which it should be connected is also accepted from the user.
  - While adding nodes, comparison will be done so that there would be no node duplication.

- **Outputs:**
  - Then we identify the source and the destinations


Number of node limit in topology
Get the node name Port number
System Name
Check already
available
Yes
DataBase
No
Updated to node information database
Check the node
limit Exceed
No
Yes
Finish the Topology Construction


PC-PT
System A
PC-PT
System C
PC-PT
System E
PC-PT
System F
PC-PT
System B
PC-PT
System D

Module 2:

- BGP (Border Gateway Protocol)Construction:
  - The BGP is Maintain itself a small network groups like LAN, wan etc.
  - The BGP is used to find the possible way to reach the destination by Applying policies.
  - The BGP is mainly used to find the best path to reach the destination and the best path is updated in the routing table.
  - Each node only selects and propagates to neighbors a single best route to the destination, if any. Both the selection and the propagation of best routes are governed by locally defined routing policies.
  - Two distinct sets of routing policies are typically employed by a node: ***Import policies*** and ***Export policies***.
  - ***Neighbor-specific import policies*** are applied upon routes learned from neighbors, whereas ***Neighbor-specific export policies*** are imposed on locally selected best routes before they are propagated to the neighbors.
  - In general, import policies can affect the "desirability" of routes by modifying route attributes.
  - Let r be a route (to destination d) received at v from node u. We denote by import (v <- u) [{r}] the possibly modified route that has been transformed by the import policies.
  - The transformed routes are stored in v's routing table.
  - The set of all such routes is denoted as candidateR (v, u);
  - CandidateR (v, d) = {r: import (v <- u) [{r}]
  - Here, N (v) is the set of v's neighbors.
  - Among the set of candidate routes candidateR (v, d); node v selects a single best route to reach the destination based on a well-defined procedure. To aid in description, we shall denote the outcome of the selection procedure at node v, that is, the best route, as bestR (v, d) which reads the best route to destination d at node v.

- Having selected bestR (v, d) from candidateR (v, d) v then exports the route to its neighbors after applying neighbor-specific export policies.
- The export policies determine if a route should be forwarded to the neighbor and if so, they modify the route attributes according to the policies.
- We denote by export (v <- u) [{r}] the route sent to neighbor u by node v after node v applies the export policies on route r.

- **Introduction:**

The BGP is used to find the possible way to reach the destination by Applying policies. Each node only selects and propagates to neighbors a single best route to the destination, if any. Both the selection and the propagation of best routes are governed by locally defined routing policies.

- **Inputs:**

Topology constructed in the previous module is the input to the current module.

- **Processing:**

Using different routing policies the best path to the destination is selected .

- **Outputs:**

The best path obtained is the output to the current module.

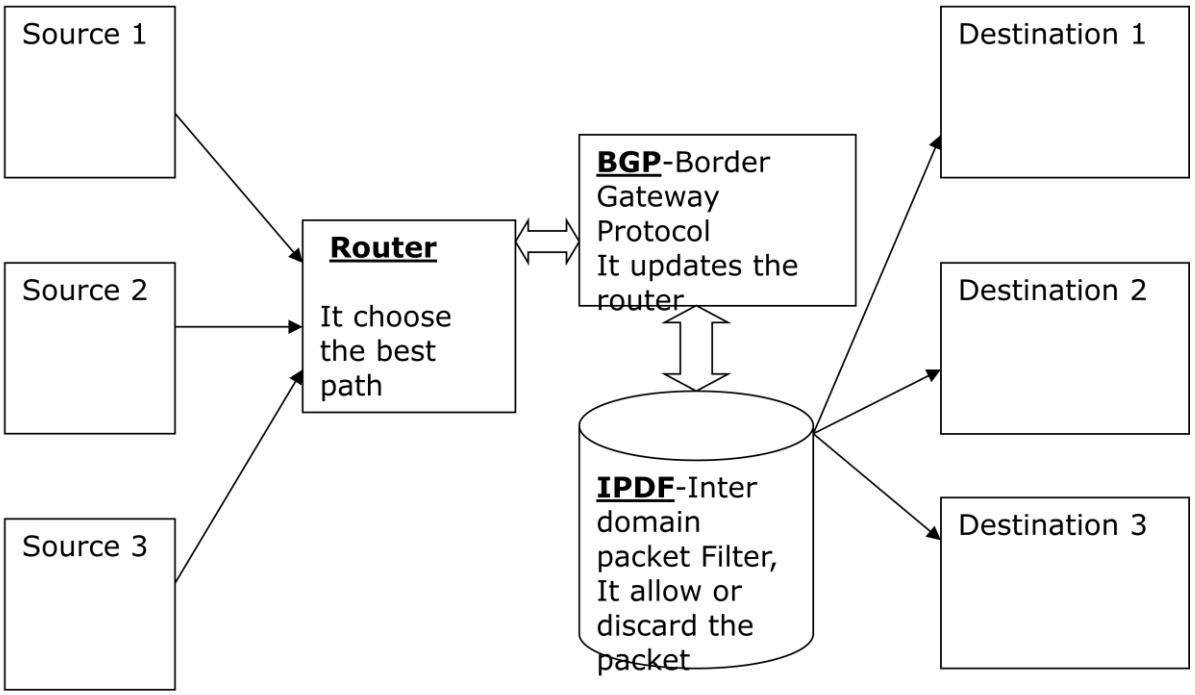
Module 3: **IDPF Construction**:

- **Introduction:**
  - The IDPF is used to check the message before it will enter into the destination.
  - The IDPF will check the source address whether it's correct or its spoofed.
    - All other packets are identified to carry spoofed source addresses and are discarded at the border router of the AS.

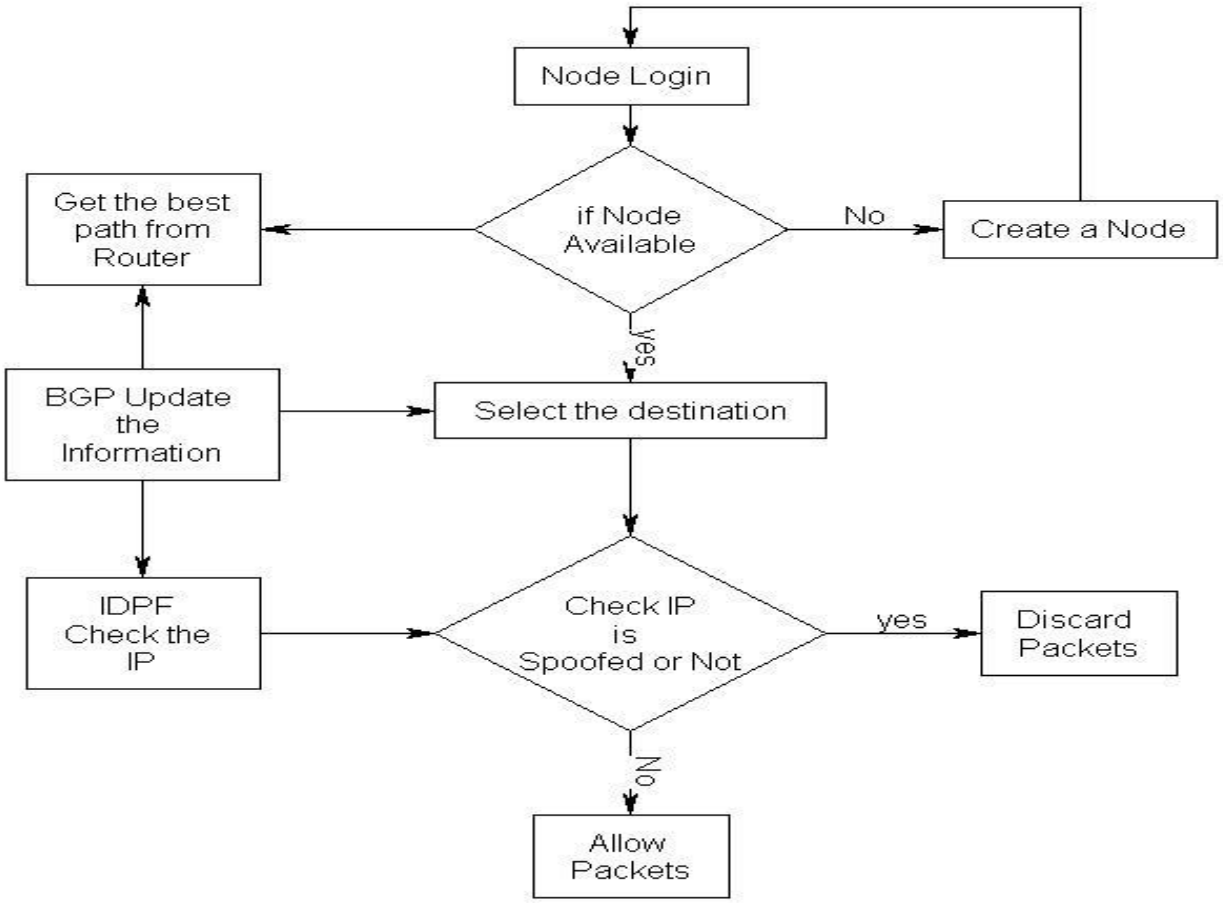
- **Input:**
  - The BGP updates obtained in the previous module is the input to the current module.
- **Processing:**
  - IDPFs can independently be deployed in each AS. IDPFs are deployed at the border routers so that IP packets can be inspected before they enter the network.
  - By deploying IDPFs, an AS constrains the set of packets that a neighbor can forward to the AS: a neighbor can only successfully forward a packet M (s, d) to the AS after it announces the reachability information of s.
- **Output:**
  - The Inter-domain packet filter acts as a Gateway and verifies the path in which then packets are coming .

Module 4:

- **Control the Spoofed Packets**:
  - Based on the IDPF we will identify the packet will be spoofed or correct.
  - If its correct the message allow to the destination or its spoofed means the packets will be discarded.



Data Flow Diagram:



Conclusion:

- In this project, we have proposed and studied IDPF architecture as an effective countermeasure to the IP spoofing- based DDoS attacks. IDPFs rely on BGP update messages exchanged on the Internet to infer the validity of source address of a packet forwarded by a neighbor. We showed that IDPFs can easily be deployed on the current BGP-based Internet routing architecture.

References:

- [1] R. Beverly and S. Bauer, “The Spoofer Project: Inferring the Extent of Internet Source Address Filtering on the Internet,” Proc. First Usenix Steps to Reducing Unwanted Traffic on the Internet Workshop, July 2005.
- [2] S. Kandula, D. Katabi, M. Jacob, and A. Berger, “Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds,” Proc. Second Symp. Networked Systems Design and Implementation, 2005.
- [3] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, “Inferring Internet Denial-of-Service Activity,” ACM Trans. Computer Systems, vol. 24, no. 2, May 2006.