Passive IP Trace back using Border Gateway Protocol (BGP)

S. Philomina, M.Jasmin R. Balaji S

Abstract*: Nowadays networks are becoming credential due to its robustness, reliability and flexibility. It got evolved with the high latency networks comprises of several workstations. Many routed protocols like IP and IPv6 are responsible to transmit the data traffic across remote network. Another factor in allocating logical address is to identify the physical address of the host in the local network. It is mandatory to allocate the IP address to transmit the data in the network. This cause the intruders to trespass into the network. They are classified as many types but we are dealing with spoofers. Our intention is to identify the spoofer's location and to eradicate them by using overlay network. In this paper, we will discuss about the existing works and our proposed method.

Keywords* : IP Traceback, Spoofing, Overlay network, Distributed Denial of Service (DDOS), Computer network management.

I. INTRODUCTION

Internet is the decentralized wide area network. It is either acquired by enterprises which are known as enterprise network. Other type is the utilization of the internet by various organisations. This is called as intranet. Usually organisations are working by using intranet which also allows the outsiders from autonomous systems. If the outsiders are intended for the good motives then it is productive for the respective organisation. But the outsider is to steal the information from the network then it is not appreciated. To prevent the network from the intruders, the intense topology with high way privacy were built. Later this solution becomes mediocre due to intervention of dark web. Hence IEEE developed many standards and protocols. Most of the countries followed these methodologies. Other Streams from European countries also started many standard committees (SC). This drastically improved the network architecture and increases the benefits of the company and their clients. Another promising attire many dedicated protocols for network security are introduced. Nowadays hackers are very crafty in dealing with these networks. They will let the spoofers to scout the network and then these spoofers will identify and inform the weak spot in the network to the intruder. Then they will break into the network. In this paper we are going to discuss about the spoofing activity and our proposed solution to get rid of them. In section II, will explain the concept of spoofing [1] and the existing solutions with their shortcomings. Later in section III, we will go through our proposed work in dealing with spoofers. Then the simulation of our work will be shown in section IV. At the end we conclude with our future works.

Revised Manuscript Received on July 22, 2019.

S. Philomina, Assistant professor /ECE , Bharath university of Higher education and Research Chennai, Tamilnadu. Email: philomina.november83@gmail.com

M.Jasmin, Assistant professor /ECE , Bharath university of Higher education and Research Chennai, Tamilnadu, Email: rifriz@gmail.com

R. Sathya Narayan, ECE , Bharath university of Higher education and Research Chennai, Tamilnadu.

Balaji S, Assistant professor /ECE , Bharath university of Higher education and Research Chennai, Tamilnadu. Email: bala.sripathy@gmail.com

II. LITERATURE SURVEY

A. Background

A spoofer is an intruder who will experience the liabilities of the host present in the network. But he can able to steal encryption standards which plays a vital role in sharing the information in the premises. But what is the use of consuming the privilege of the host? It is a root cause for the severe attacks like DNS amplification attacks [2], SMURF and synchronization flooding and generic network breakdowns etc.

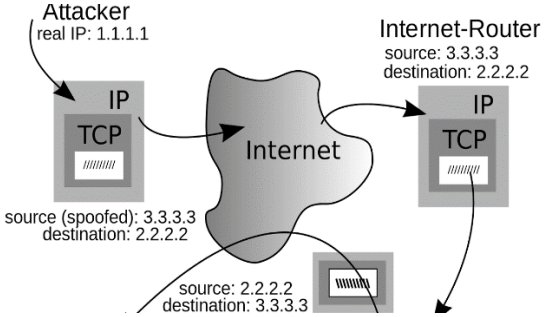


Figure1: IP Spoofing through forged IP address

From the above figure 1.1, the spoofer will enter into the network by using forged IP address. Generally, organisations will allocate the IP addresses to their hosts by the request made to Internet service provider (ISP). The ISP will get the IP clusters from Regional Internet Registry (RIR). IANA (Internet Assigned numbers authority) is the head of this IP network which is located atUSA [3]. They will segregate their regions by the continental basis. So Asian pacific is responsible for providing IP address for Asian countries. From them our national internet registry (NIR) will get IP patterns which are obtained and converted to the series of IP address. This IP patterns are the key for the spoofers who will identify them by simple systematic. This is

enough to enter into the network by the forged IP address.

The spoofing activity is regular in today's networks. This is due to lack of surveillance in public networks. This will make the impostors to break the network and its system.

The question of the hour is whether these activities can be monitored predominantly, the answer is yes. We can able to watch out these spoofing attacks with some preventive calculations. But the problem is even the plug in and out, proxy usage of the employees will also consider as the generic spoofing. It seems like funny but it is habitual in today's ASA firewalls [4].

B. Motivation

To trace out the spoofers is a feasible task. It needs a dedicated people to witness the spoofers without hype in it.

But to ensure this we need a technique to drag him out of the progress before it is sustained. With this in mind, many solutions were introduced to the legacies and often faced many consequences by its counterparts. The common part they face is the bandwidth utilisation of the real environment. Hence our ultimate goal is to provide a solution with a negligence of bandwidth utilisation.

Real network with Anti-proxy agent.

Certain methodologies like packet logging and packet marking [5] are mostly declared in routers with its internetwork capabilities. But it is difficult to cult it in massive fashion. Then comes the ICMP trace back [6] which is despicable for the excessive use of bandwidth and traffic overhead. Thirdly the link testing [7] is the alternate for the foreseen approaches due to the lack of virtual setup. Yet it is dreadful in dealing with internet level. Finally, the disruption of the spoofers by taking down in three-way handshake [8] by means of change of contention window is appreciated. Still they cannot disclose the location of the spoofer. Another important thing to remember is that these approaches needs ASEs to cooperate at vendor level which is unattainable in practical site. And the collaboration of ISP's to achieve the trace backs is meaningless.

C. Aim

The existing mechanism either needs the drastic change in topology of the network or deployment of the high latency networking devices. Both of them are compelling to the organisation in order to retain the mediocre attacks. Our purpose is to provide a solution with full-fledged heftiness and also cost effective. Another thing is our solution is supple with any platforms.

The concept of overlay network is brainchild of our work. We design them to deal the incoming spoofers and eradicate them. But this not possible until we ensure that the incoming host is a spoofer. To detect them we use the following mechanisms.

1. Queue Timer.
2. Link Mapping.
3. Hash Creation.
4. Anti-Proxy agent.
5. Received Signal Strength.

The detection of spoofers is crucial because it may cause burden to the organisation. Hence these approaches will accurately detect them. Then we have to find the intention of spoofer. This is the bonus of our work lies here. You will get to know soon.

The last step is to disclose the location of the spoofer and disregard him. The passive IP Trace back approach is applied here in a lighter vein. The reason is the real network do not involve in our method which is an advantage for us.

III. PROPOSED WORK

Our work is quite different from previous trace back mechanisms in approaching the spoofers. The usual mindset of the admin is to protect the network from attackers.

This raises the amount of attacks to the network. Most networks abide by egress filtering which is filtering the malicious node from invading the network. This filtering is accomplished by edge router.

We follow ingress filtering and divert them to the overlay network. This will impeccably reduce the repetitive attacks to the network.

The real network is responsible for the network traffic. The edge router will forward the packets from the access points or from the autonomous system. The normal traffic will not interrupt during the process. Secondly the real network will receive the logs about the attacks at time periods. This is essential for the host to understand the vulnerability of their network. Finally, the anti-proxy agent available in real network monitors the workstations in the network and also to detect the spoofer. They work based on character schemes like application, flow rate and behaviour etc. It is illustrated in figure 1.2.

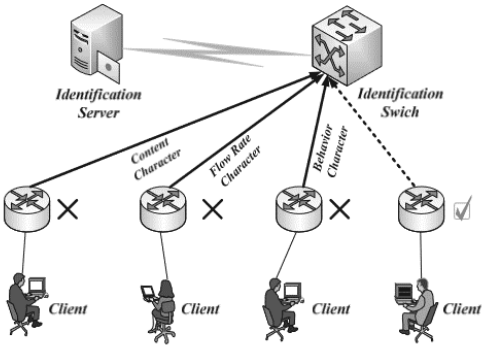


Figure2: Anti Proxy mechanism using characters

D. Virtual Network

The setup of virtual network is similar to TCP, IP Layer in networks. They are doppelganger of the real network with the exact parameters including the subnets. They are connected virtually with special tracking router using loopbacks [9]. Their role is to treat and eat the spoofers. The components present in overlay networks are isolated logically.

The edge router will divert the spoofed packet to the virtual network and the special tracking router will request the NAS to which data it should provide to the spoofer.

The Network attached storage is conventional when compared to generic Intel server. They provide large capacity with plug-in facility. This makes the administrators to reduce the workload. The network attached storage will have the

duplicate fake databases which will be provided to spoofers. The databases with their respective keys will be available in common authentication procedures. This is the preliminary detection of the spoofer.

E. Locality Of Spoofer

Generally Spoofers are originated from two sites. One is within their campus or from the autonomous system. The major contribution of our work is to identify their spot of direction.

The attack signatures and data cookies are used to specify the work spot of the spoofer. Then the concept of inaccessible hop count is also under consideration. The spoofer will be less than ten hops to the edge routers.

F. HASH Generation

Another technique is sequence gap present in the HASH frames. These frames are generated by all nodes during the data transmission. The syntax of the HASH is CPU id, Computer name, **creation time of the frame (Sequence number).** The last field will get incremented for individual nodes. If the spoofer gets intruded into the real network, the sequence number will revive again.

G. Sassy Approach

Our approach is a redux from the existing passive IP trace back. The routing protocol we are using here is BGP (Border Gateway protocol) [10]. This protocol holds good for the autonomous system. The spoofer is detected with our schemes and he will be diverted to the overlay network. It comprises of a virtual circuit and a network attached storage. The virtual circuit acts as kernel which decides the parameters to be executed. Then after retrieving the request from the spoofer, first it will find the discovers the location of the spoofer by Err-ICMP packets. Then it will influence the NAS to provide the fake databases with other duplicate datasets like CPU id, Location and router id. The spoofers frames will be identified using suspicion mark [11] in it.

This makes the spoofer to believe that he is in the right network. Up to this phase, only his coordinates will be found. The block diagram of sassy approach is shown in figure 1.3.

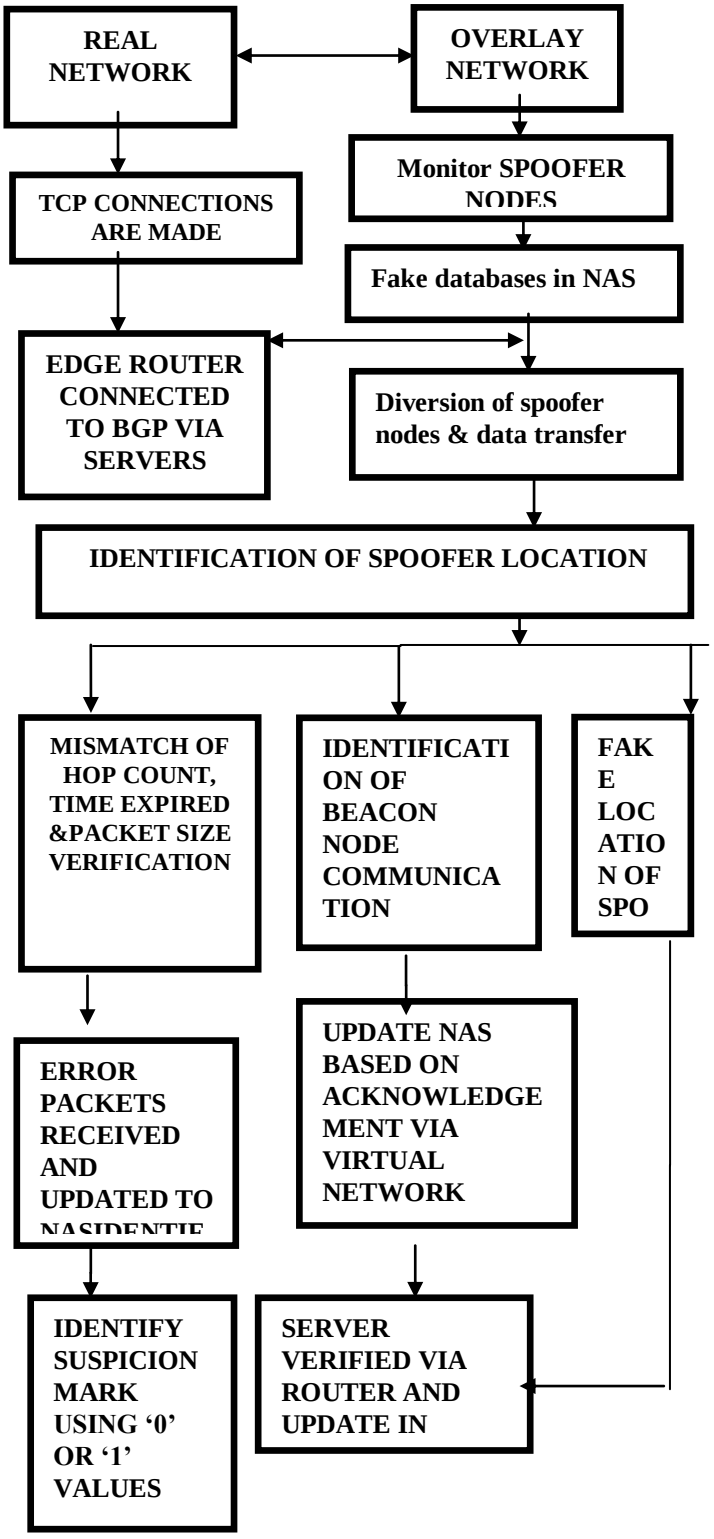


Fig 3: Block diagram of SASSY Approach

Phase I

Before completing the transfer, the NAS will initiate a query regarding the change in new window change [12]. This means the host has to enter the new speed in bps. This mandatory for every secure transmission even in real network. From this input we can check whether the spoofer is within the campus or from autonomous system.

Phase II

In this stage the spoofer will

receive his stuffs. Our next motive is to eliminate him. For this we use the hyper loops [13] as invoice after the data transfer which will create multiple loop files to his system. During our process the queue timer and proxy check will be active to monitor the network. If the spoofer distrust the transmission and open the data then he will receive the triggered hyper loops. The hyper text of loop file creation is shown in figure 1.4.

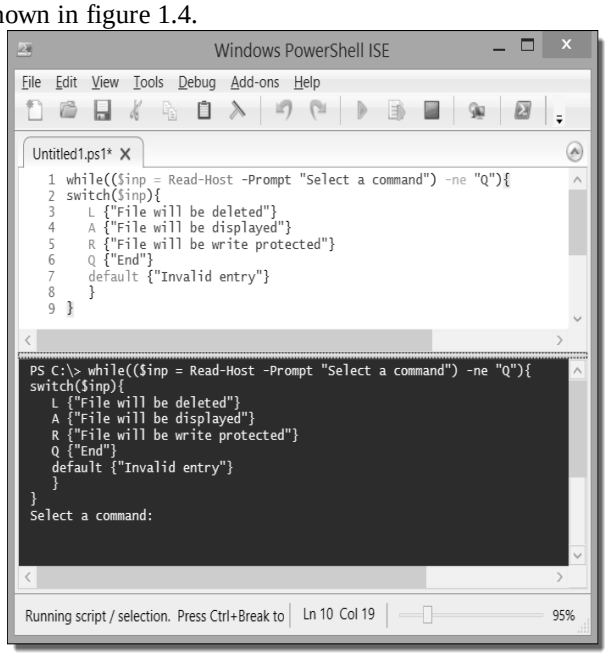


Fig 1.4 Creation of Hyper text

Phase III

Suppose the spoofer is not requesting the data but simply available in the network. In this case we send him the Error recovery time interval. Here the spoofer should enter the lasting time. If he keyed the correct time interval, then he will be witnessed as the intra spoofer. This is the final verification for the work-spot of the spoofer. On other hand the network will monitor the beacon nodes [14] at periodic interval.

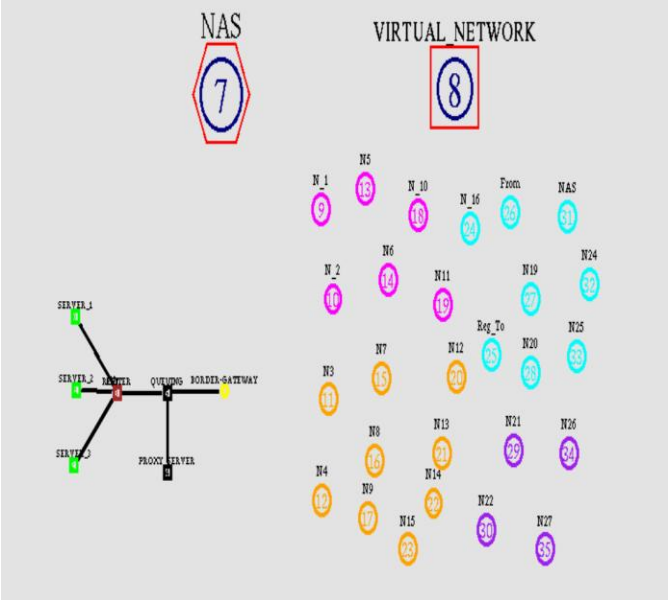
IV. SIMULATION

Our simulation is done using NS2 with renewed source codes. We have analysed the major trimming issues appeared in CAIDA dataset. The simulation is shown in figure 1.5

```
# ======================================================================
# Define options
# ======================================================================

set opt(chan)       Channel/WirelessChannel         ;# channel type
set opt(prop)       Propagation/TwoRayGround        ;# radio-propagation model
set opt(netif)      Phy/WirelessPhy                 ;# network interface type
set opt(mac)        Mac/802_11                      ;# MAC type
set opt(ifq)        Queue/DropTail/PriQueue         ;# interface queue type
set opt(ll)         LL                              ;# link layer type
set opt(ant)        Antenna/OmniAntenna             ;# antenna model
set opt(ifqlen)         20000                          ;# max packet in ifq
set opt(nn)             8                           ;# number of mobilenodes
set opt(adhocRouting)   BGP                    ;# routing protocol
set opt(threshold)  1.41828e-20         ;# the distance of coverage 250m
set opt(x)          1000                            ;# x coordinate of topology
set opt(y)          500                              ;# y coordinate of topology
set opt(stop)       50000                              ;# time to stop simulation
set num_wired_nodes     6
set num_bs_nodes        1               ;# this is not really used here.
set tcp         Sack1
set win         5
```

Figure4: I. datasets II. Simulation of sassy approach.



For demonstration purpose, we isolated the overlay network to display their construction.

V. CONCLUSION

In our paper we discussed about the concept of spoofing with their existing solution. Sassy approach is reliable in means of bandwidth utilisation, less load to clients and exact precision. Apart from these reasons we are trap the spoofers with overwhelming effects. This will tremendously reduce the spoofing attack and meanderingly reduces major security attacks. Our next maxim is to implement this design in other mesh networks with less dependencies.

REFERENCES

1. Detecting SYN Flooding Agents under Any Type of IP SpoofingDalia NashatXiao Hong JiangIEEE 2008.
2. DNS Amplification Attacks: Alert (TA13-088A) us-cert.gov 2013.
3. The IANA Functions: An Introduction to the Internet Assigned Numbers Authority iana.org 2008.
4. Cisco Adaptive Security Appliance (ASA) Software cisco.com 2016.
5. Passive IP Traceback: Disclosing the Locations of IP Spoofers from Path Backscatter Guan Yao IEEE 2015.
6. Novel hybrid schemes employing packet marking and logging for ip traceback, B. Al-Denarii and M. Govender's, IEEE2006.
7. Improved EAACK: Secure Intrusion Detection System Sharad Awatere IEEE 2012.
8. A Mitigation model for TCP SYN flooding IP Spoofing L. Kavi Shankar 2011.
9. Understanding the Loopback Interface documentation juniper.net 2017.
10. Bhatia, B. AODV based Congestion Control Protocols: Review IJCSIT 2016.
11. Real Time Implementation of k fake Location Generation Algorithm to Location Privacy in Location Based Services Ms. Apurva K. Kina IEEE 2017.
12. The UCSD Network Telescope in brief caida.org 2015.
13. Emanuel Goldberg and Knowledge Machine processingBuckland, Michael IEEE 2006.
14. An Anti-PROXY Detecting Scheme Based on Characters Shawna Sun Nan Wang IEEE2011.

AUTHORS PROFILE

S. Philomina, Assistant professor /ECE , Bharath university of Higher education and Research Chennai, India

M.Jasmin* Assistant professor /ECE , Bharath university of Higher education and Research Chennai,India

Balaji .S , Assistant Professor , ECE, Bharath Institute of Higher Education and Research,Chennai,India