December 2019

DATAPLANE-BASED DISTRIBUTED DENIAL-OF-SERVICE (DDOS) MITIGATION AND SPOOFING PREVENTION VIA SEGMENT ROUTING OVER INTERNET PROTOCOL VERSION 6 (SRV6) NETWORK PROGRAMMING

Bruce McDougall

Karthik Kumaravel

Dave Clough

Meghan McGinn

Recommended Citation

McDougall, Bruce; Kumaravel, Karthik; Clough, Dave; and McGinn, Meghan, "DATAPLANE-BASED DISTRIBUTED DENIAL-OF-SERVICE (DDOS) MITIGATION AND SPOOFING PREVENTION VIA SEGMENT ROUTING OVER INTERNET PROTOCOL VERSION 6 (SRV6) NETWORK PROGRAMMING", Technical Disclosure Commons, (December 02, 2019)
https://www.tdcommons.org/dpubs_series/2728

DATAPLANE-BASED DISTRIBUTED DENIAL-OF-SERVICE (DDOS) MITIGATION AND SPOOFING PREVENTION VIA SEGMENT ROUTING OVER INTERNET PROTOCOL VERSION 6 (SRV6) NETWORK PROGRAMMING

AUTHORS:
Bruce McDougall
Karthik Kumaravel
Dave Clough
Meghan McGinn

ABSTRACT

Techniques described herein augment packet tagging Distributed Denial-of-Service (DDOS) mitigation solutions with a powerful anti-spoofing capability. A Segment Routing over Internet Protocol (IP) version 6 (SRv6) network programming technique is proposed herein wherein authenticated sessions are given an SRv6 header to append to all outbound packets. Traffic with the valid SRv6 header is allowed to pass thru the service provider network whereas all other traffic destined to the victim of the DDOS attack is dropped. The valid SRv6 header address can be rotated from amongst the 18, 446, 744, 073, 709, 551, and 616 possible addresses found in a /64 IPv6 subnet, thus making it nearly impossible to spoof the valid SRv6 address.

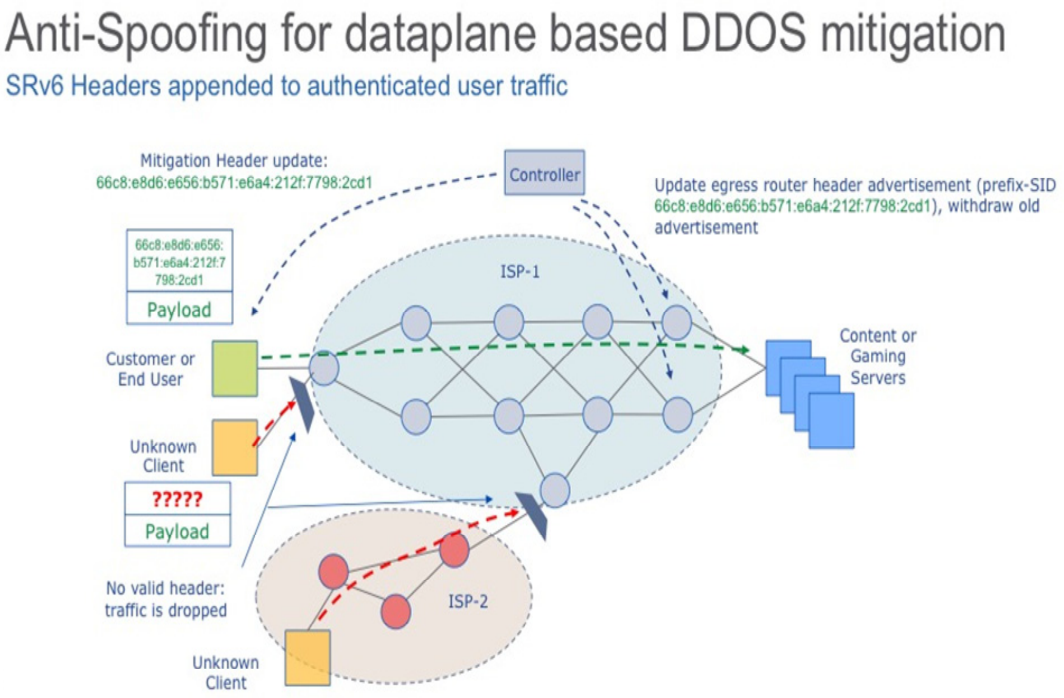
DETAILED DESCRIPTION

Any organization with an online presence can be subject to a Distributed Denial-of-Service (DDOS) attack. Traditionally, DDOS detection and mitigation techniques involve Central Processing Unit (CPU) intensive processes that try and sort valid traffic from attack traffic by comparing signatures and examining different attributes of the traffic, and then creating deep packet inspection filters to block the traffic. These implementations tend to be centralized, and therefore subject to DDOS themselves, and often require costly specialized hardware.

Dataplane-based DDOS mitigation solutions have the potential to deliver very high performance at low cost, however, they are subject to potential spoofing by malicious actors.

Published by Technical Disclosure Commons, 2019

The solution proposed herein augments packet tagging DDOS mitigation solutions with a powerful anti-spoofing capability. In particular, this proposal provides a SRv6 network programming technique in which authenticated sessions are given a SRv6 header to append to all outbound packets. Traffic with the valid SRv6 header is allowed to pass thru the service provider network whereas all other traffic destined to the victim of the DDOS attack is dropped, as illustrated in Figure 1, below.



Anti-Spoofing for dataplane based DDOS mitigation

SRv6 Headers appended to authenticated user traffic

Mitigation Header update:
66c8:e8d6:e656:b571:e6a4:212f:7798:2cd1
Controller
Update egress router header advertisement (prefix-SID 66c8:e8d6:e656:b571:e6a4:212f:7798:2cd1), withdraw old advertisement
66c8:e8d6:e656:b571:e6a4:212f:7798:2cd1
Payload
ISP-1
Customer or End User
Content or Gaming Servers
Unknown Client
?????
Payload
No valid header: traffic is dropped
ISP-2
Unknown Client

Figure 1

The valid SRv6 header address can be randomly rotated from amongst the 18, 446, 744, 073, 709, 551, and 616 possible addresses found in a /64 IPv6 subnet. Once the new SRv6 header has been distributed to authenticated users, the packet dropping filters are updated to allow the new header to pass and drop all other traffic.

The packet dropping filters can be automatically generated and distributed to all nodes around the outer edges of the network via network automation tooling, which provides a highly distributed, and therefore highly scalable architecture for mitigation.

An additional benefit of this proposal is its ability to operate across network domains or autonomous systems. For example, a service provider offering the DDOS mitigation service can advertise the SRv6 /64 subnet across Autonomous System Number (ASN) or domain boundaries. The SRv6 address itself is a valid IPv6 address and therefore a downstream domain or ASN would forward traffic to the destination subnet so long as it complies with that ASN's respecting routing policy.

It is possible that a malicious actor could learn the valid SRv6 header and distribute it to their botnet. To address this proposal provides for rotating the valid SRv6 header using the SRv6 network programming locator/function structure, as illustrated in Figure 2, below.

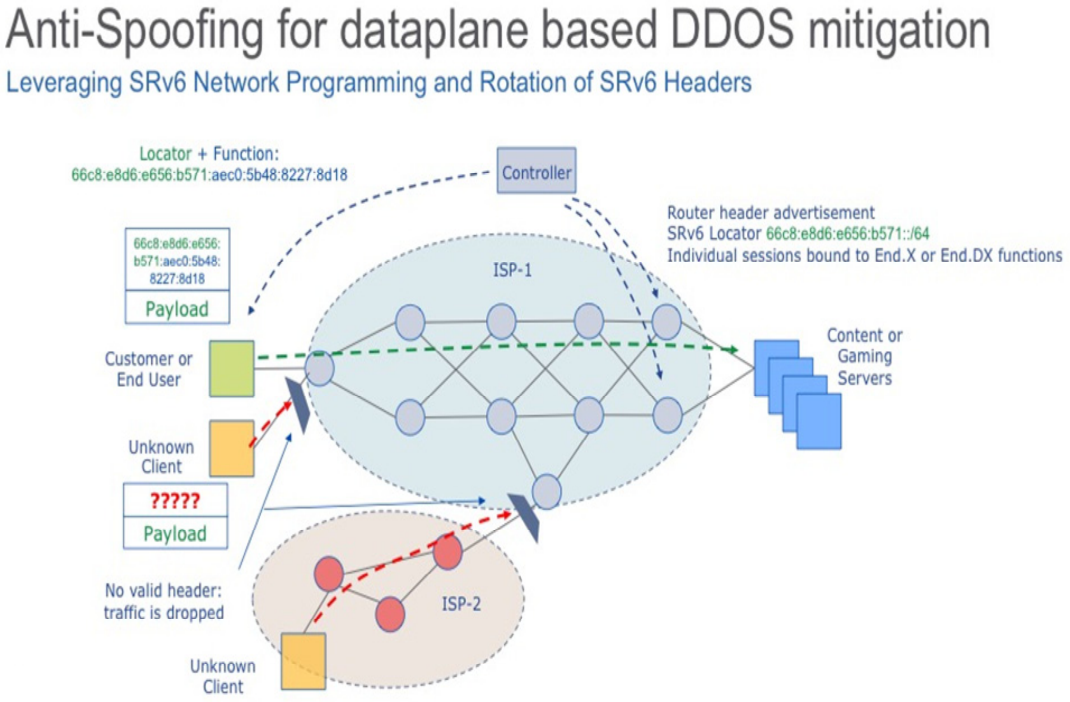

Anti-Spoofing for dataplane based DDOS mitigation
Leveraging SRv6 Network Programming and Rotation of SRv6 Headers
Locator + Function:
66c8:e8d6:e656:b571:aec0:5b48:8227:8d18
Controller
66c8:e8d6:e656:
b571:aec0:5b48:
8227:8d18
Payload
Router header advertisement
SRv6 Locator 66c8:e8d6:e656:b571::/64
Individual sessions bound to End.X or End.DX functions
ISP-1
Customer or
End User
Content or
Gaming
Servers
Unknown
Client
?????
Payload
No valid header:
traffic is dropped
ISP-2
Unknown
Client

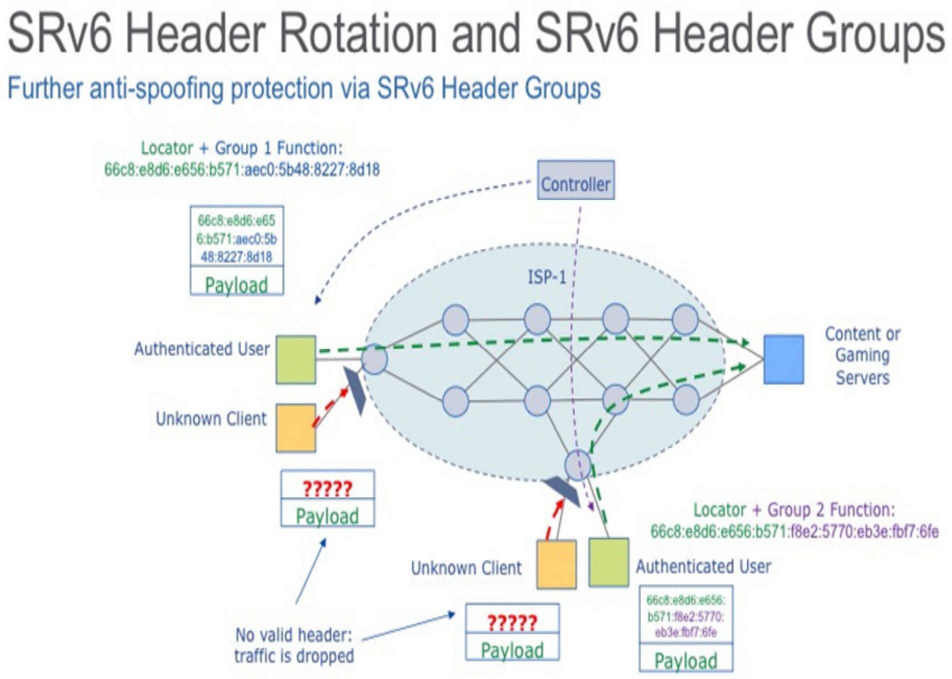
Figure 2

For this feature, the SRv6 locator (subnet) remains the same and the individual IPv6 address rotates using a randomly chosen value in the function /64 portion of the subnet. Rotating the valid SRv6 address (or addresses) from amongst such a massive pool provides a strong anti-spoofing capability. In some implementations, the address rotation itself could be provided on a regular or random time interval. This anti-spoofing capability could only be broken if a malicious actor managed to:

1. Sniff a valid user's packets on the network
2. Capture the valid SRv6 header, and then

3. Develop a technique to distribute the valid header information to enough bots to use in their attack before the next header rotation occurs.

An operator may have the option of assigning a single SRv6 header from the /64 block for all authenticated users. Or the service provider could assign different SRv6 addresses within the /64 block to groups of users based on geographic location, customer ID range, subscriber tier, or other status. The grouping technique is illustrated in Figure 3, below.



SRv6 Header Rotation and SRv6 Header Groups

Further anti-spoofing protection via SRv6 Header Groups

Figure 3

The grouping technique may provide additional protection against a malicious actor sniffing packets and distributing the valid header information throughout their botnet as this involves the actor to also know the SRv6 header grouping technique (e.g., by geography, customer ID, etc.) and develop some mapping technique to associate the proper SRv6 header to the appropriate bot(s).

This proposal may provide advantages over 802.1x, which does not work over the Internet. In particular, this proposal provides for appending authenticated sessions with Internet routable SRv6 (IPv6) headers; thus, all routers (edge, transit, etc.) may participate in forwarding or enforcement. Further, this solution operates in the dataplane, thereby providing line rate performance at a very high scale and is enforced at the network edge such that the solution may not involve firewalls or other appliance-based middle boxes.

Thus, this solution provides an Internet-routable SRv6 header-ID method, which allows traffic from authenticated nodes to bypass Access Control Lists (ACLs) or other filters at the network edge.

The techniques presented herein could also be augmented by Unique Identifier (UID) rotation and grouping tools. For example, if an authenticated node becomes compromised, the SRv6 ID rotation and location grouping techniques described herein may allow detection systems to narrow down attack sources. Once identified, the attack sources could simply not be given an updated SRv6 ID on the next key rotation. In some implementations, unique identifiers could be offered for regions and then if there is an attack, the identifiers could be more granularly changed to isolate the bad systems.

In some implementations, unique filtering can be applied during setup such that Internet of Things (IoT) devices would need to authenticate and append traffic with an appropriate SRv6 UID tag. Thus, the techniques presented herein may provide additional value to IoT technologies as embedded headers may provide a user/operator the ability to perform packet tracing and/or other debugging tasks.

Accordingly, this dataplane-based DDOS mitigation plus anti-spoofing solution provides greater scale, nearly unbreakable anti-spoofing, and the automated distribution of traffic filters to all edge nodes provides much faster response to DDOS attacks than current solutions on the market.

In summary, techniques herein provide for the ability to augment packet tagging DDOS mitigation solutions with a powerful anti-spoofing capability. A SRv6 network programming technique is proposed in which authenticated sessions are given a SRv6 header to append to all outbound packets. Traffic with the valid SRv6 header is allowed to pass thru the service provider network whereas all other traffic destined to the victim of the DDOS attack is dropped. The valid SRv6 header address can be rotated from amongst the 18, 446, 744, 073, 709, 551, and 616 possible addresses found in a /64 IPv6 subnet, thus making it nearly impossible to spoof the valid SRv6 address.