DDoS Detection and prevention System Using eBPF

Overview

- DDos Detection
  - Algorithms for detection of the malicious traffic
  - Probabilistic Count
  - Usage of eBPF
- DDoS Mitigation
  - Usage of Express Data Path
- Conclusion

DDoS Detection and Mitigation eBPF with XDP

Detection

DDoS Attack Detection Algorithms Based on Entropy Computing

- Research by National University of Singapore, Singapore.
- Anomaly based detection technique.

Works with a sample of data to check the distribution of packets source IP. Then calculates entropy the formula for which is:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

Where H is entropy,
pi is the emergence probability of each distinct source IP address and n is the number of packets.

More entropy = Higher probability of DDoS

Great for volumetric DDoS.

Not so great for low entropy attacks, striking a balance between FRR and FAR rates with entropy is challenging.

Low-Rate DDoS Attack Detection Using Expectation of Packet Size

- Research by School of Mathematics and Computer Science, China
- Anomaly based detection technique.

The low-rate DDoS packets are purposely created by prebuilt programs therefore the features of these packets are highly similar.

Additionally, for the purpose of best-effort transmission of attack packets, attackers usually generate small packets or even empty packets to reduce the resources required.

while, in contrast, although the packets of communication protocols are also small, packets filled with user data are normally large.

The packet sizes of communication protocol packets in legitimate traffic are small in the daily Internet 62 bytes for SYN. ACK is 60 bytes.

User data traffic packets are usually the max size (HTTP traffic) 1500 bytes

The study observed that the attack packets had very low packet sizes, therefore concluding DDoS

Great for Protocol Based DDoS (SYN Flood) but not so great for Application layer DDoS

Approximate Heavy Hitters and the Count-Min Sketch

- CS168: The Modern Algorithmic Toolbox Lecture, Stanford University
- Anomaly based detection technique.

Solve the problem of Heavy Hitters;

An array A of length n, and also a parameter k. Think of n as very large (in the hundreds of millions, or billions), and k as modest (10, 100, or 1000). The goal is to compute the values that occur in the array at least n/k times.

Solution?

Use Count Min Sketch Data structure to provide a fixed, sublinear storage to process A and find Approx count of values.

D = number of non cryptographic hash functions
W = no. of digits of the output of the hash function

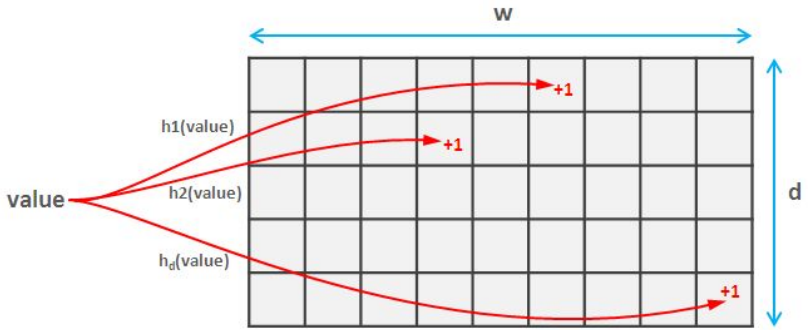
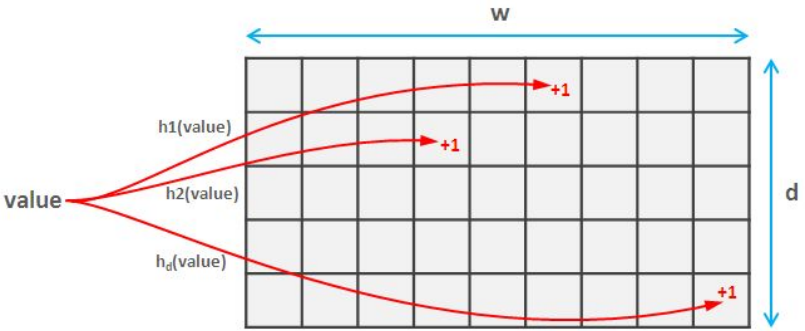


Figure: Visual Representation of the CMS Data Structure

Count Min Sketch

Insert:

- Structure initialized with zeros
- Each stream input goes through the hash functions
- Output of hash function determines the column
- that needs to be updated in the structure.
- Increments of 1.

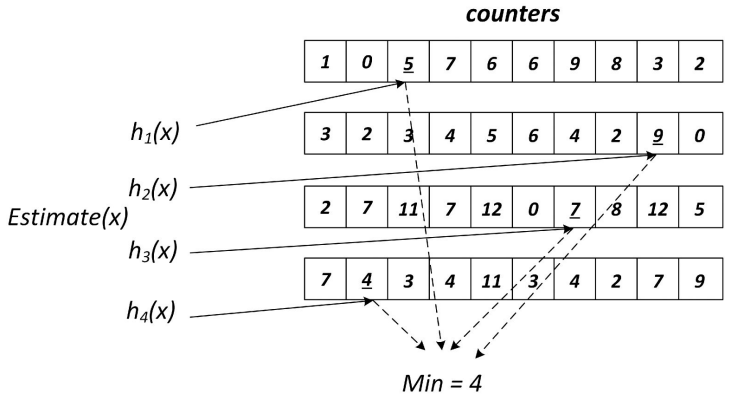


Count:

- Pass value to hash functions
- O/p of hash functions determines the locations
- Obtain values at locations. Choose minimum.

Advantages:

- Size of the structure independent of input
- Lossy count with no under-counting.



Mitigation

XDP - Express Data Path

eXpress Data Path provides a high performance, **programmable** network data path in the Linux kernel.

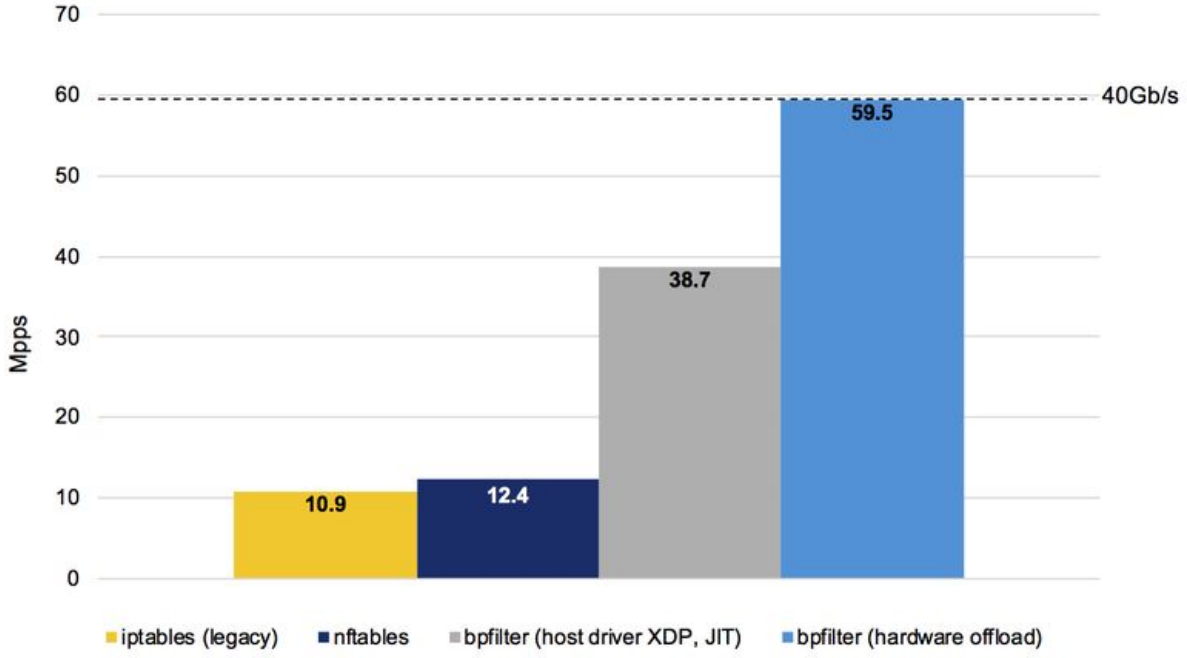
XDP provides bare metal packet processing at the lowest point in the software stack which makes it ideal for speed without compromising programmability.

Can be implemented dynamically with the integrated fast path without kernel modification.

eBPF can be used to write XDP programs.

Trusted Technology - Used by Cloudflare, Facebook, Netronome, Prometheus, and many more.

Performance Comparisons

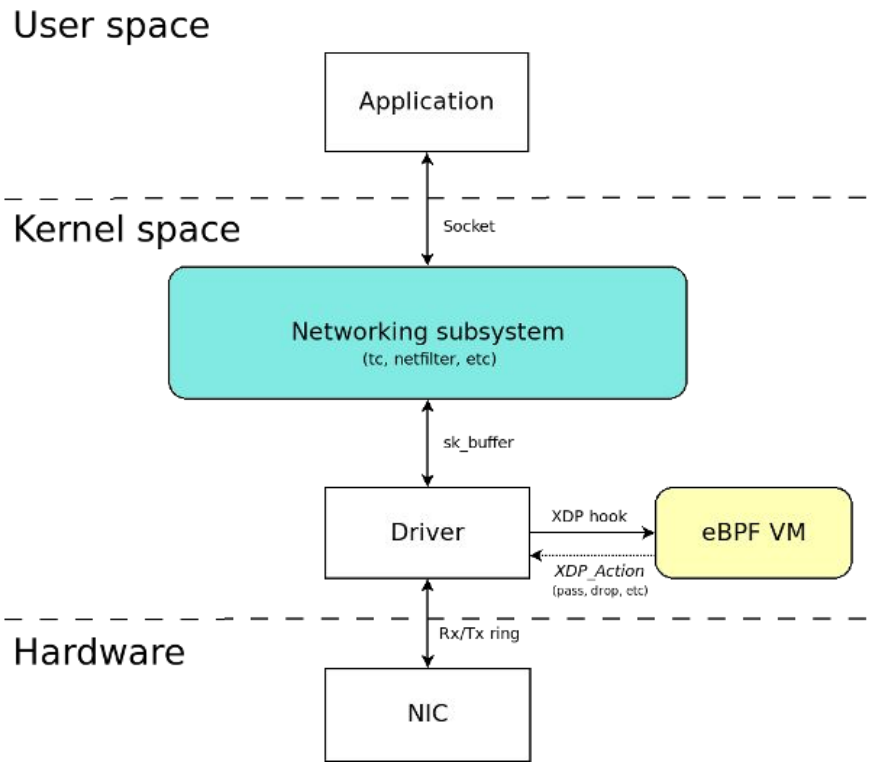


graph as presented by Quentin Monnet at FRnOG 30

Packet Flow

Ring Buffers: Ring buffers are shared buffers between the device driver and Network Interface Card (NIC). These buffers store incoming packets until the device driver can process them. Ring buffers exist on both the receive (rx) and transmit (tx) side of each interface.

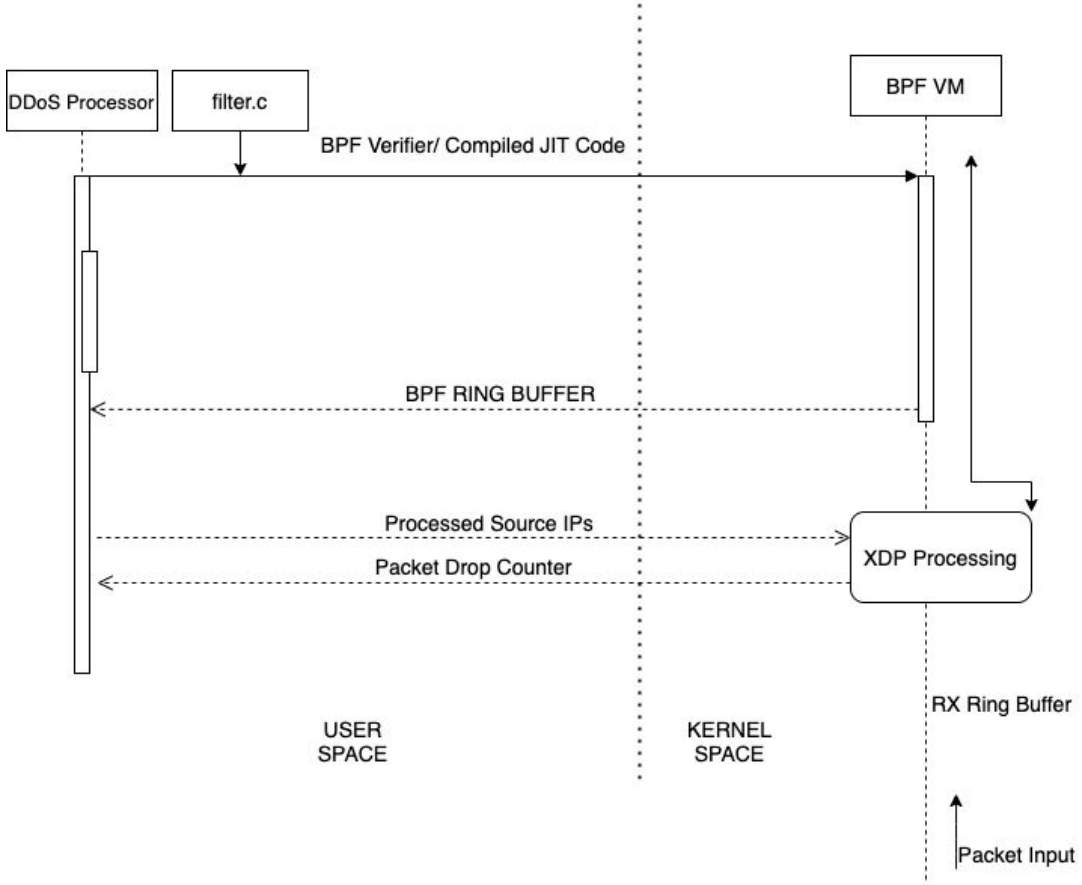
eBPF VM: Register-based Virtual Machine using a custom 64 bit RISC instruction set capable of running Just-in-Time native-compiled "BPF programs" inside the Linux kernel with access to a subset of kernel functions and memory. It is a full VM implementation, not to be confused with the Kernel-based VM (KVM) which is a module enabling Linux to act as hypervisor for other VMs. It is also part of the mainline kernel



Architecture

Heavy Hitters Estimation

Clean Pipe Approach



DEMO

Screenshots

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 xdpgeneric/id:74 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:84:68:e4 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.79.5/24 brd 172.16.79.255 scope global dynamic noprefixroute ens33
       valid_lft 61656sec preferred_lft 61656sec
    inet6 fe80::7b04:ac3b:7d3:cdf7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
Collecting packet sample, count at 2099 packets so far
DDoS Mitigation in effect! 3219118 packets dropped so far
Source IP: 7.79.16.172 with total packets identified before confirm DoS: 2096
performing DDOS mitigation...
IPs sent to XDP for mitigation!
Possibly lost 228977 samples
Collecting packet sample, count at 2133 packets so far
DDoS Mitigation in effect! 3450225 packets dropped so far
Drop Rate: 23056.6093988 pkts/sec
```

Advantages

- Lightweight
- Dynamic
- Protocol Independent

Disadvantages

- Not a Silver Bullet
- Drop rate visibility
- Volumetric DDoS/ IP entropy Issues

Improvements

- Time-bound sample of 1M packets. If Sample does not reach the set size in set amount of time, No DDoS.
- Feedback loop to clear old entries.
- Dynamically control threshold for heavy hitters.
- Feed Live stream to Count Min Sketch.
- Combine various DDoS Detection Algorithms - Entropy, Packet Size.

References

DDoS Attack Detection Algorithms Based on Entropy Computing Paper by Liying Li, Jianying Zhou, and Ning Xiao, https://rdcu.be/cjbIS

Low-Rate DDoS Attack Detection Using Expectation of Packet Size Lu Zhou, Mingchao Liao, Cao Yuan, and Haoyu Zhang, https://www.researchgate.net/publication/320341005_Low-Rate_DDoS_Attack_Detection_Using_Expectation_of_Packet_Size

https://web.stanford.edu/class/cs168/l/l5.pdf

BPF Performance Tools by Brendan Gregg, https://www.oreilly.com/library/view/bpf-performance-tools/9780136588870/

Linux Observability with BPF by David Calavera & Lorenzo Fontana, https://www.oreilly.com/library/view/linux-observability-with/9781492050193/

Introduction to eBPF and XDP, https://www.mcorbin.fr/pages/xdp-introduction/

Netoptimizer Kernel Prototypes Project, https://github.com/netoptimizer/prototype-kernel

BCC Reference Guide, https://github.com/iovisor/bcc/blob/master/docs/reference_guide.md

Writing an XDP Network filter with BPF, https://duo.com/labs/tech-notes/writing-an-xdp-network-filter-with-ebpf

THANK YOU!