IT Security Labs

Leveraging SDN for Collaborative DDoS Mitigation

Sufian Hameed, Hassan Ahmed Khan

IT Security Labs

National University of Computer and Emerging Sciences, Pakistan

FAST-NUCES

Introduction

- The legacy of DDoS continues to grow in sophistication and volume.
- Recently, IoT devices are used to generate DDoS for millions of IPs (1.2 Tbps attack on DYN).
- Websites known as Booters offering “DDoS as a Service” has made the situation worse [1].

DDoS Defense

- Destination based DDoS defense schemes are popular due to higher accuracy and cheaper cost
- However they cannot mitigate attack on the path to the victim and waste resources

This calls for an efficient mitigation strategy to ease out network resources along the transit path of an attack from source to victim.

Push-Back DDoS Mitigation

- Push-back schemes to mitigate DDoS attack along the attack path has been discussed in the research community [14], [15].
  However,
  - They require more resources at various levels
  - The push-back mechanism must be deployed in all the participating network components (routers and switches).
  - Complexity and overhead because of the coordination adds serious management challenges.

Here SDN can promise ease of management, where a single controller can manage the coordination among all the network components at the AS level.

SDN Based DDoS Mitigation

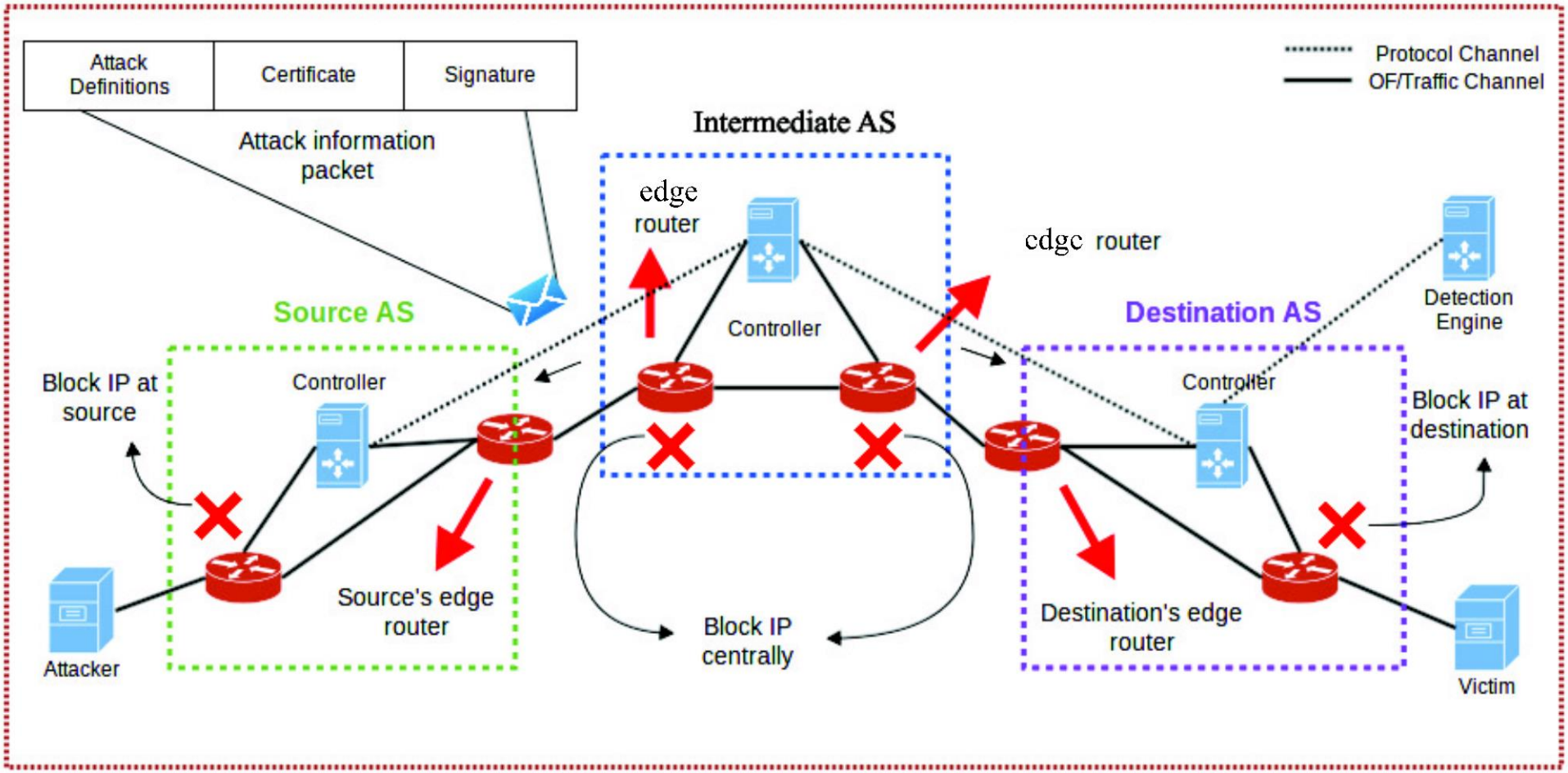
- SDN bring us new approaches to deal with DDoS attacks (destination based approaches are discussed here [7]–[13]).

- In [6], Giotis et al. proposed a push-back DDoS mitigation scheme across multiple SDN networks.
  - Embed the incident report as URIs within BGP signals.
  - BGP is very complex and hard to master.
  - Any modifications to existing protocol will challenge the deployment.
  - Incident exchange will only take place after every BGP update interval. Therefore, the report latency will increase with the number of hops.
  - No validation of incident reports exchanged among the adjacent SDN domains. This could make the whole infrastructure vulnerable to fake incident reports from malicious domains.

Contribution

- Propose a lightweight, efficient and easy to deploy collaborative DDoS mitigation scheme leveraging SDN.
- SDN controllers in different AS use a secure C-to-C communication protocol to effectively communicate and inform about an ongoing attack. Through this approach the SDN
  - Block the malicious flows within the network.
  - Inform the neighboring domains/networks about an ongoing attack.

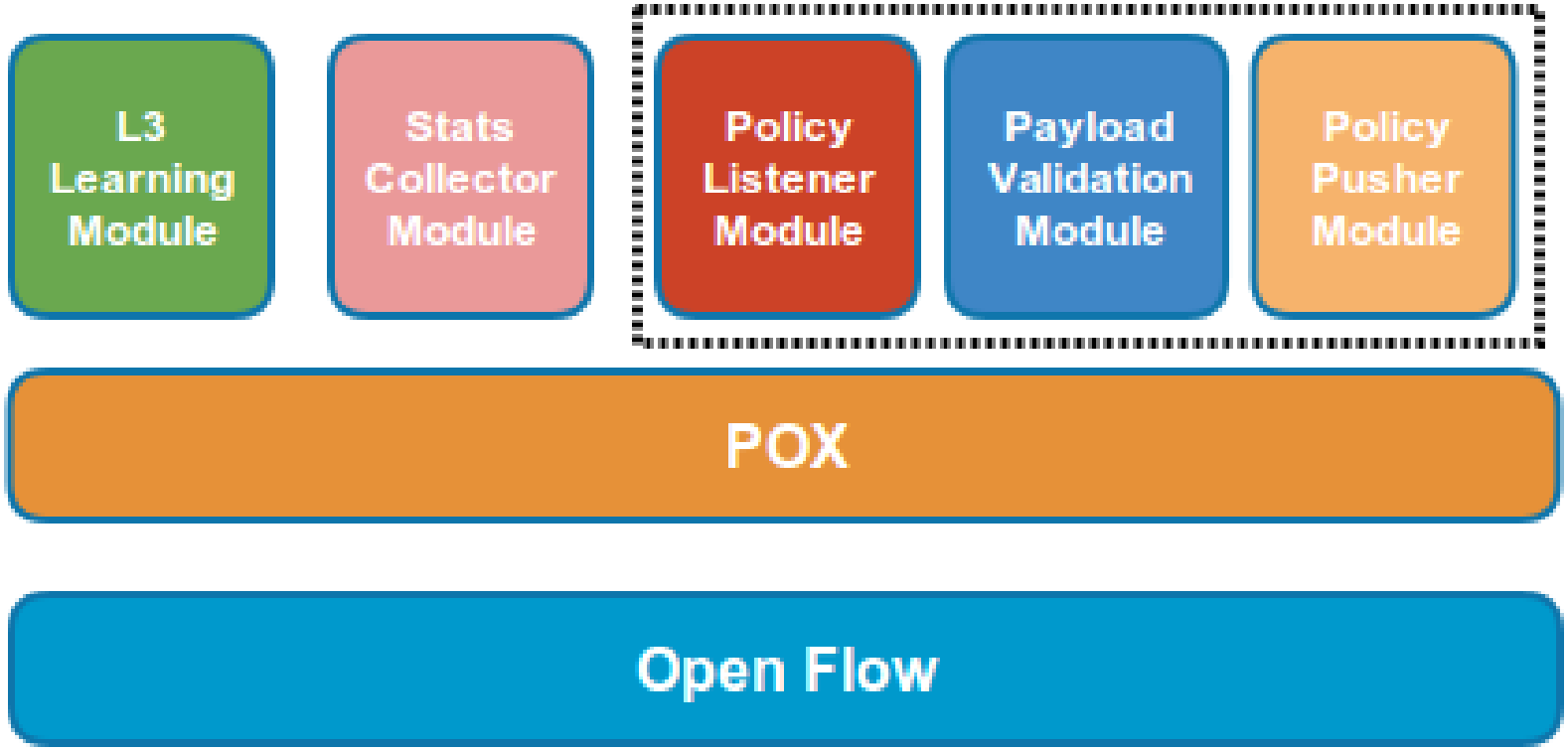
High Level Architecture



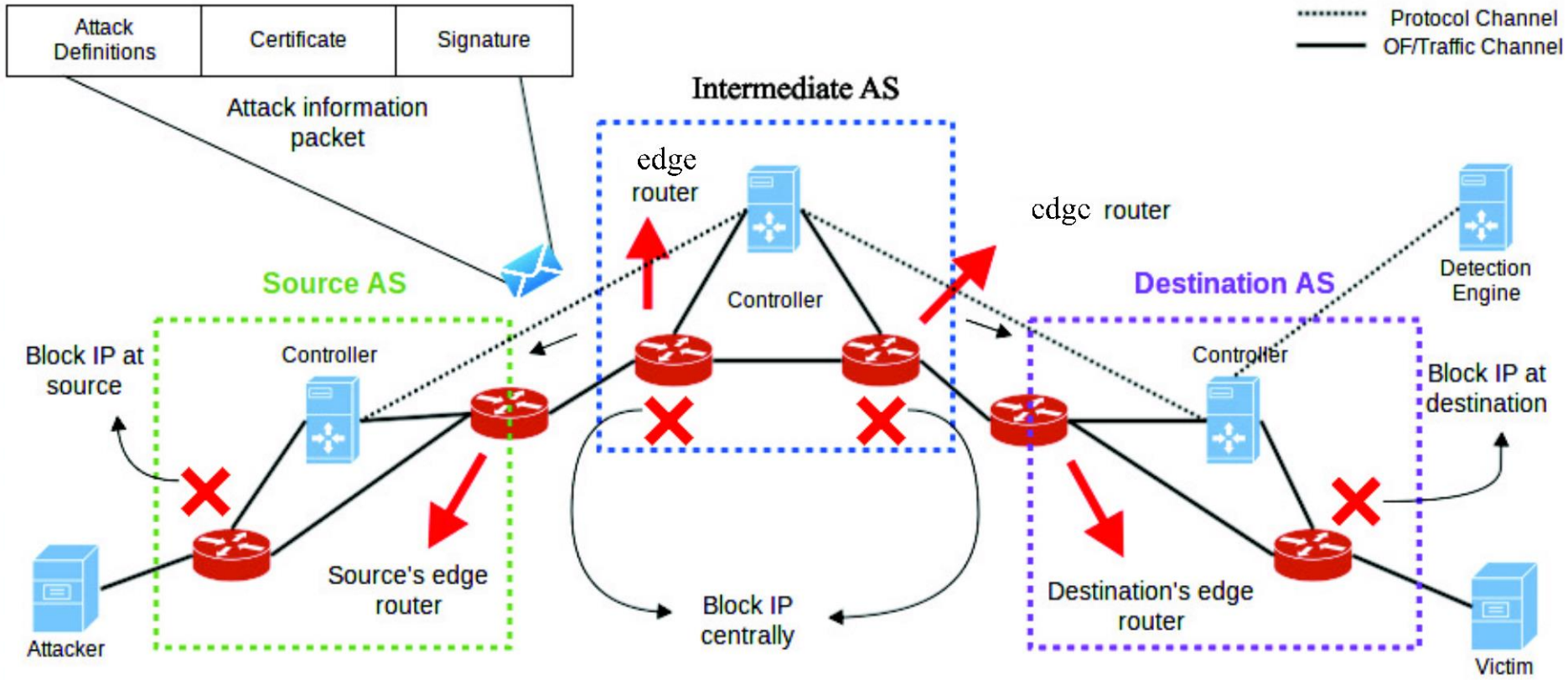
Controller to Controller Protocol (C-to-C)


```
{
  "ips": [
    "10.0.2.4",
    "12.0.23.2"
  ],
  "signature": "Base64 encoded signature string",
  "certificate": "Base64 encoded certificate"
}
```

Component Architecture of Controller



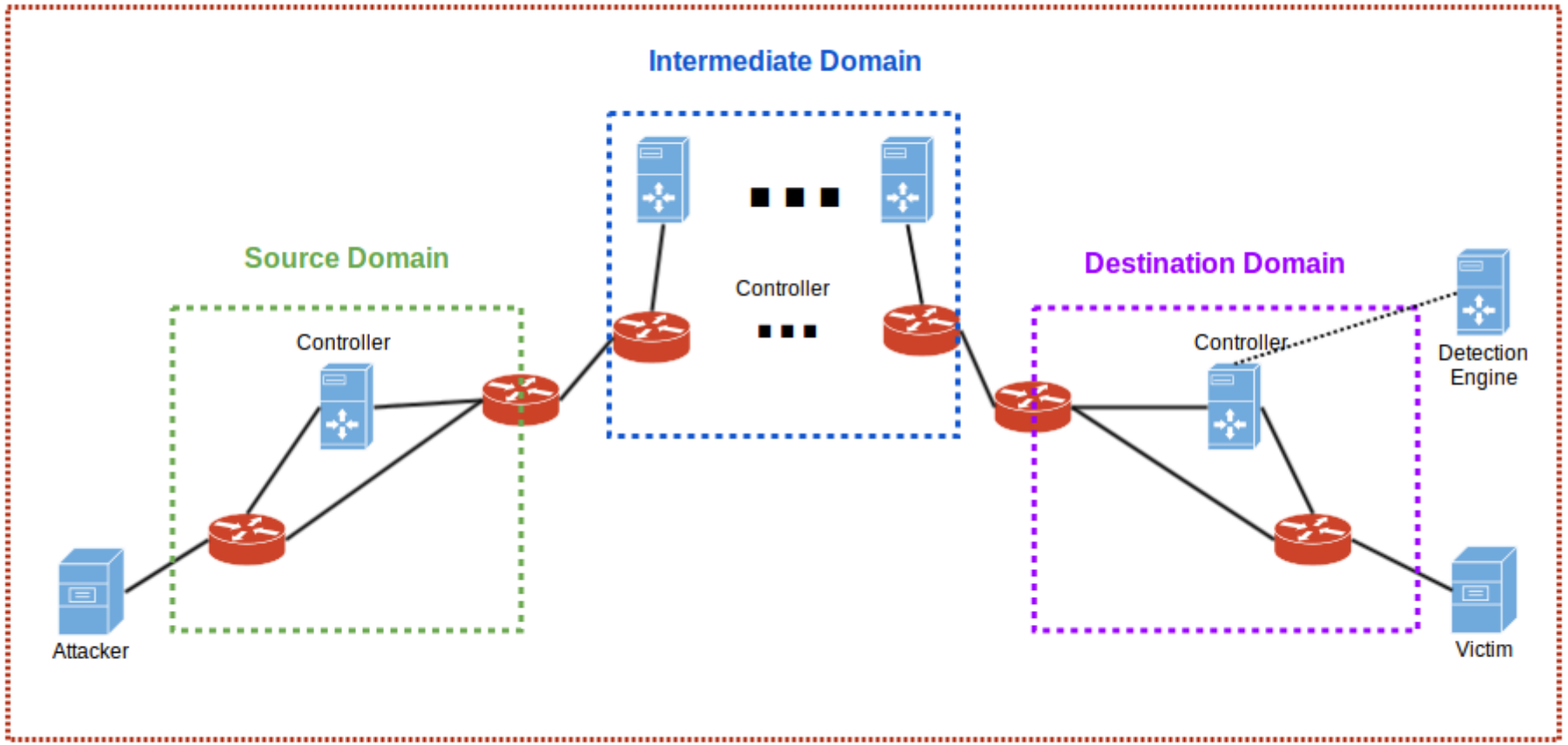
Work Flow


Attack Definitions
Certificate
Signature
Attack information packet
Protocol Channel
OF/Traffic Channel
Intermediate AS
edge router
edge router
Controller
Source AS
Destination AS
Detection Engine
Block IP at source
Controller
Controller
Block IP at destination
Source's edge router
Block IP centrally
Destination's edge router
Attacker
Victim

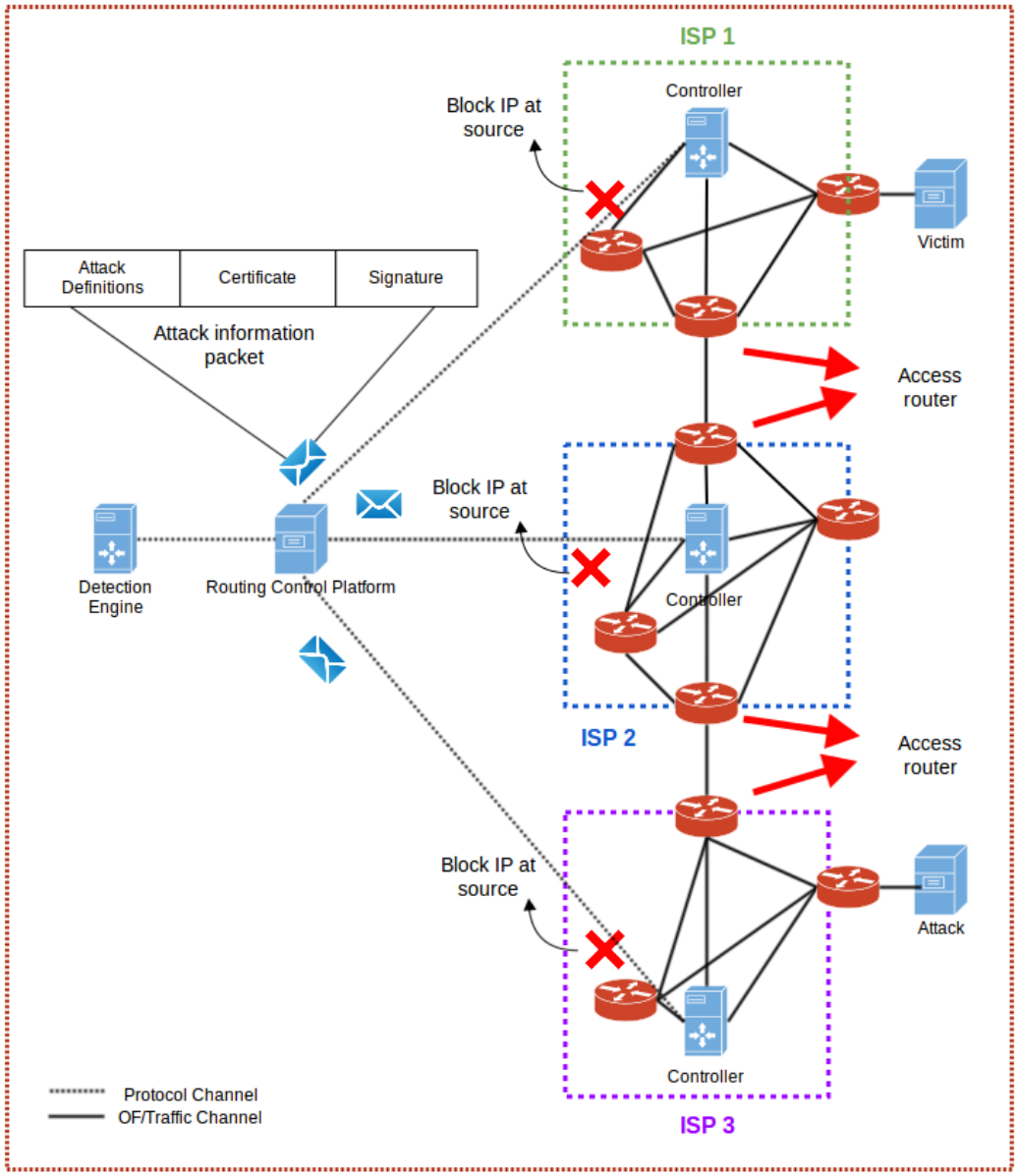
Testbed

- We use Mininet [2] to emulate the networks with POX [3] as the controller platform.
- All the Mininet instances emulating different networks are connected via GRE tunneling.
- For most part each node in our testbed consists of 2.60 GHz Intel core i5 CPU, 8 GB RAM, 500 GB HDD and 1 Gbps Ethernet card.
- Scapy [4] to generate attack and legitimate traffic.

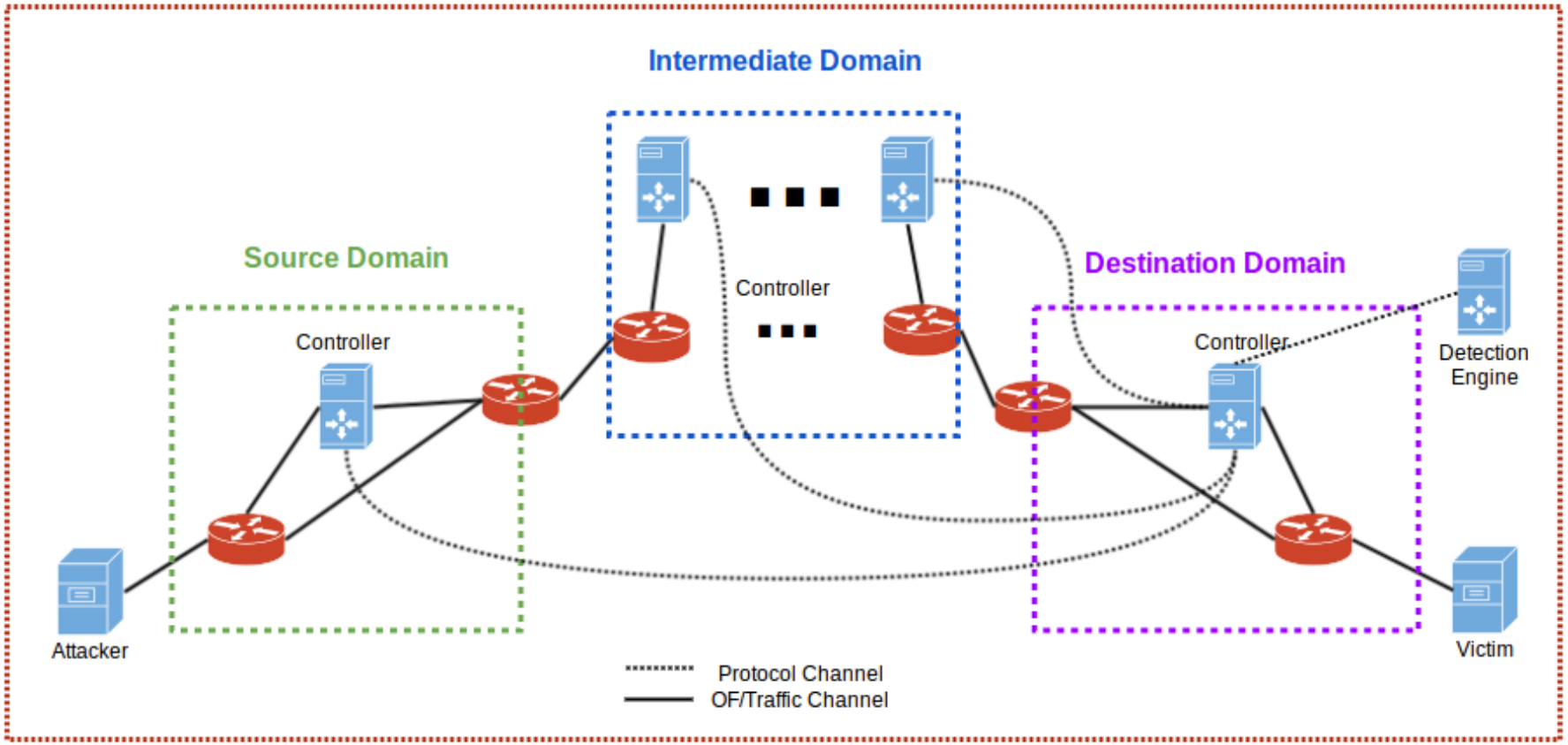
Deployment Approaches (Linear)



Deployment Approaches (Centralize)

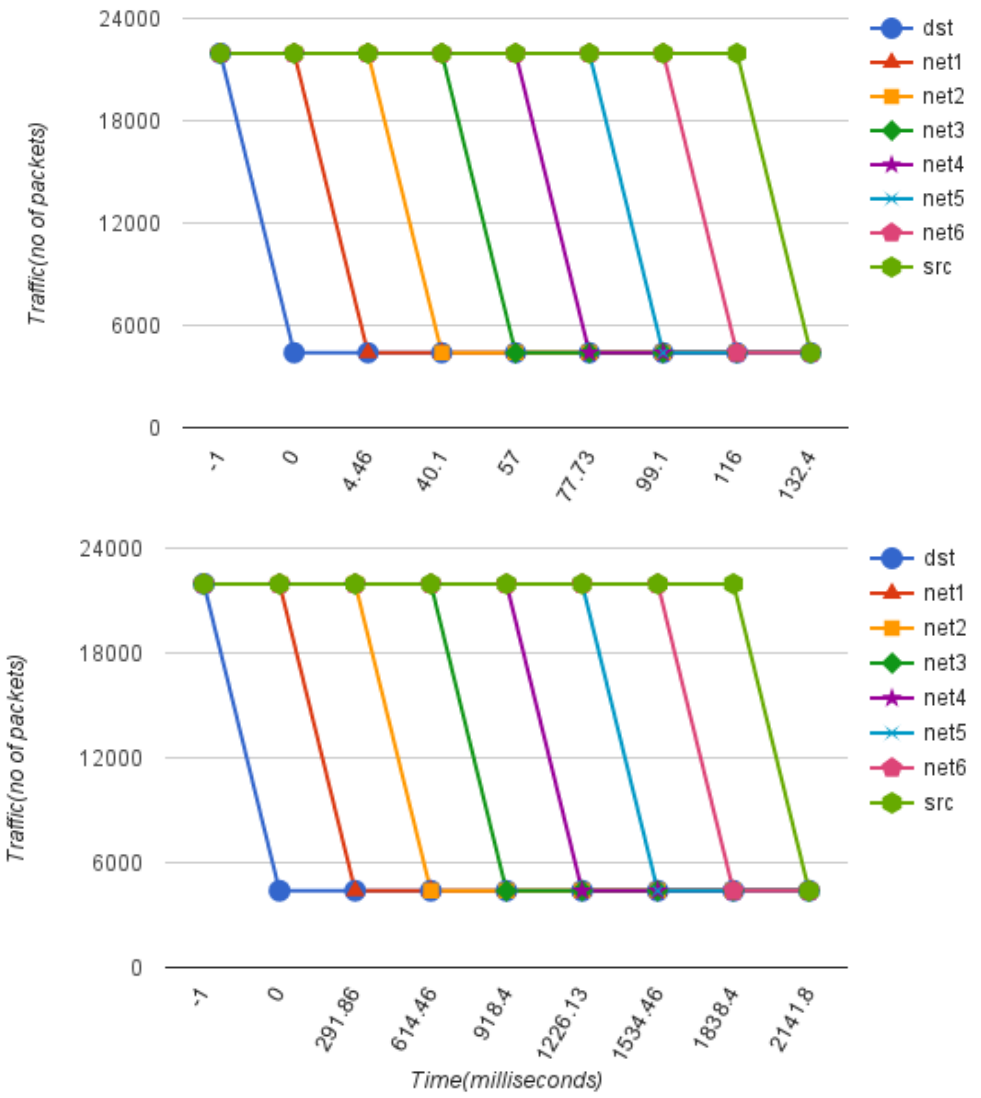


Deployment Approaches (Mesh)



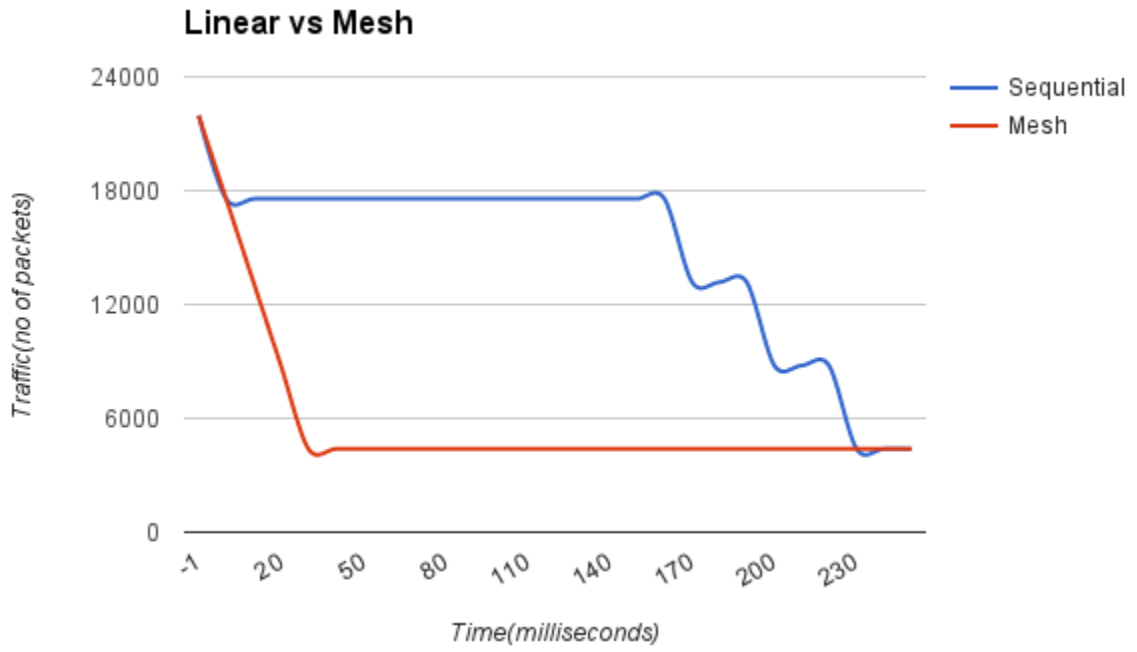
Effect on Attack Mitigation (Linear)

- 8 networks (1 src, 1 dst, 6 interim --- as per ISP settings the AS path is stable at 4.3 hops [5]).
- 21,960 pkt/secound (4,392 legit, 17,568 malicious)
- 1st experiment LAN settings with no delays and 1K attack IPs.
- 2nd experiment added AS-to-AS communication latency.
- 150 ms avg delay using a 500 Kbps Internet and 100K attack IPs.



Effect on Attack Mitigation (Mesh)

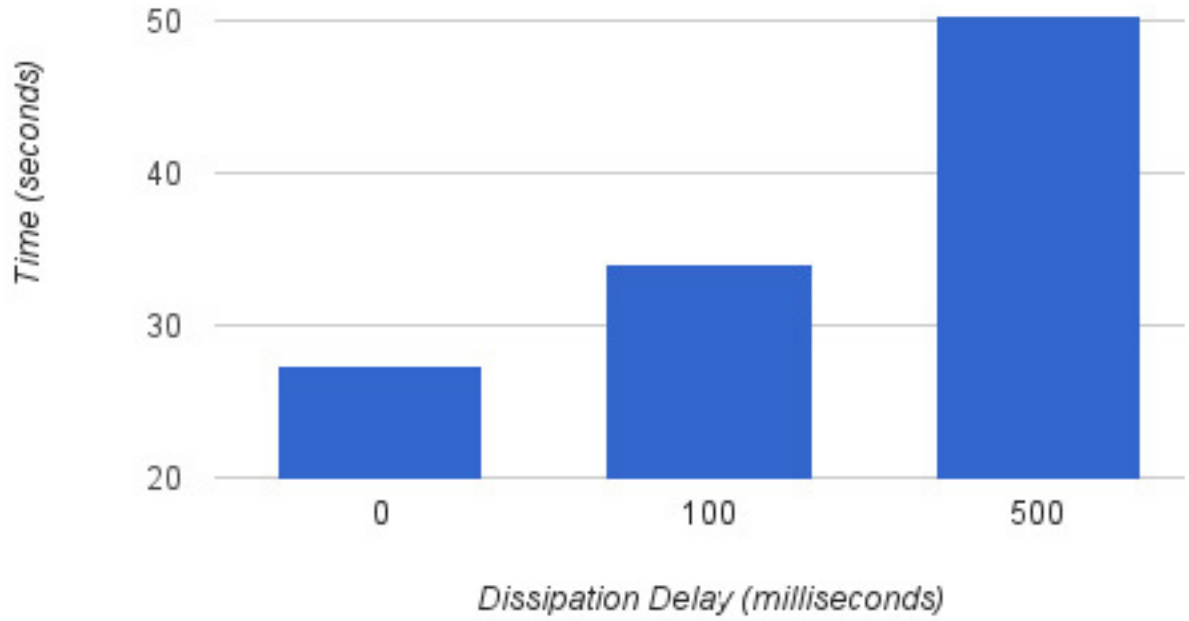
- The controller are directly and effect is immediate drop in attack traffic.



Performance of Central Control Plane

Dissemination delays of the flows.

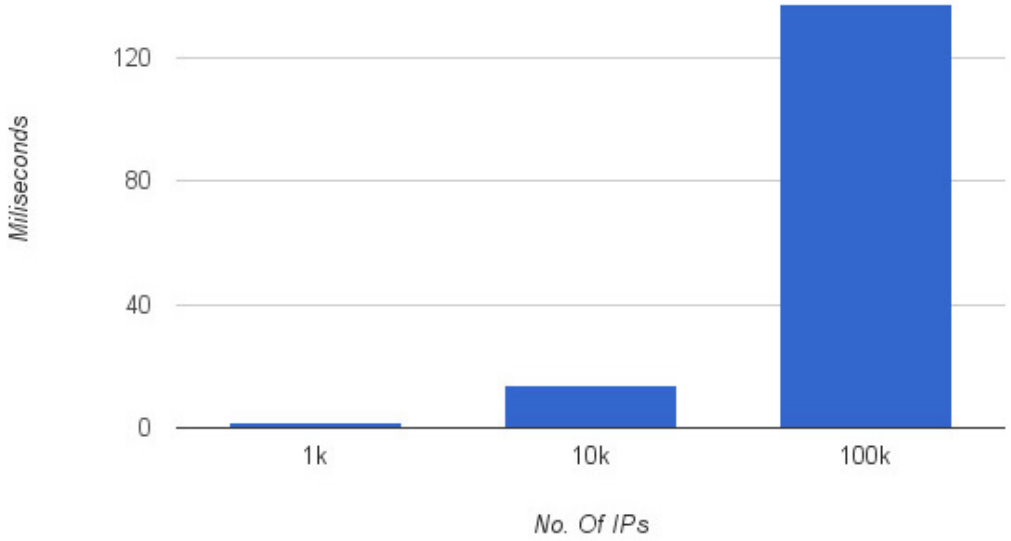
- Core i3 @ 1.70 GHz and 4 GB RAM for central controller.
- 100 different flows in Burst mode, 100ms delays and 500 ms delays (delay between two attack definitions).
- 28, 34 and 50 seconds to dissipate the flows



Performance of Central Control Plane

Payload size on Performance.

- 1K IPs, 10K IPs and 100K IPs.
- 1.8 ms, 13ms an 137 ms to process (signature verification and insertion of flow table entry) 1K IPs, 10 IPs and 100K IPs respectively.



Conclusion

- We present a lightweight, efficient and easy to deploy collaborative DDoS mitigation scheme leveraging SDN.
- Efficient propagation of attack definitions all the way from the victim to the attack sources.
- Introduced three different deployment approaches i.e. linear, central and mesh in our testbed and tested the overall efficiency.
- The effect of mitigation is instantaneously transferred from destination to source.
  - It took around 2.14 seconds to mitigate the attack in an eight hop linear deployment.
  - Only requires somewhere between 290 to 330 ms to process and forward attack definitions between adjacent networks.

References

[1] Aiko Pras et al. DDoS 3.0 - How terrorist bring down the Internet

[2] Mininet. www.mininet.org/.

[3] Pox controller. www.github.com/noxrepo/pox.

[4] Scapy. www.secdev.org/projects/scapy/.

[5] Autonomous system path lengths. https://labs.ripe.net/Members/mirjam/updateon-as-path-lengths-over-time, 2012.

[6] K. Giotis, M. Apostolaki, and V. Maglaris. A reputation-based collaborative schema for the mitigation of distributed attacks in sdn domains. In IEEE/IFIP Network Operations and Management Symposium, 2016. .

[7] M. Belyaev and S. Gaivoronski. Towards load balancing in sdn-networks during ddos-attacks. In MoNeTeC, 2014.

[8] R. Braga, E. Mota, and A. Passito. Lightweight ddos flooding attack detection using nox/openflow. In 35th IEEE LCN, 2010.

[9] Nhu-Ngoc Dao, Junho Park, Minho Park, and Sungrae Cho. A feasible method to combat against ddos attack in sdn network. In ICOIN 2015.

[10] K. Giotis, G. Androulidakis, and V. Maglaris. Leveraging sdn for efficient anomaly detection and mitigation on legacy networks. In Third European Workshop on Software Defined Networks, 2014.

References

[11] J. Jeong, J. Seo, G. Cho, H. Kim, and J. S. Park. A framework for security services based on software-defined networking. In Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on, 2015.

[12] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yang. A sdn-oriented ddos blocking scheme for botnet-based attacks. In Sixth International Conference on Ubiquitous and Future Networks (ICUFN), July 2014.

[13] Q. Yan and F. R. Yu. Distributed denial of service attacks in softwaredefined networking with cloud computing. IEEE Communications Magazine, April 2015.

[14] Xiaowei Yang, David Wetherall, and Thomas Anderson. A dos-limiting network architecture. In ACM SIGCOMM Computer Communication Review, volume 35. ACM, 2005.

[15] Xiaowei Yang, David Wetherall, and Thomas Anderson. Tva: a doslimiting network architecture. IEEE Transactions on Networking, 2008.