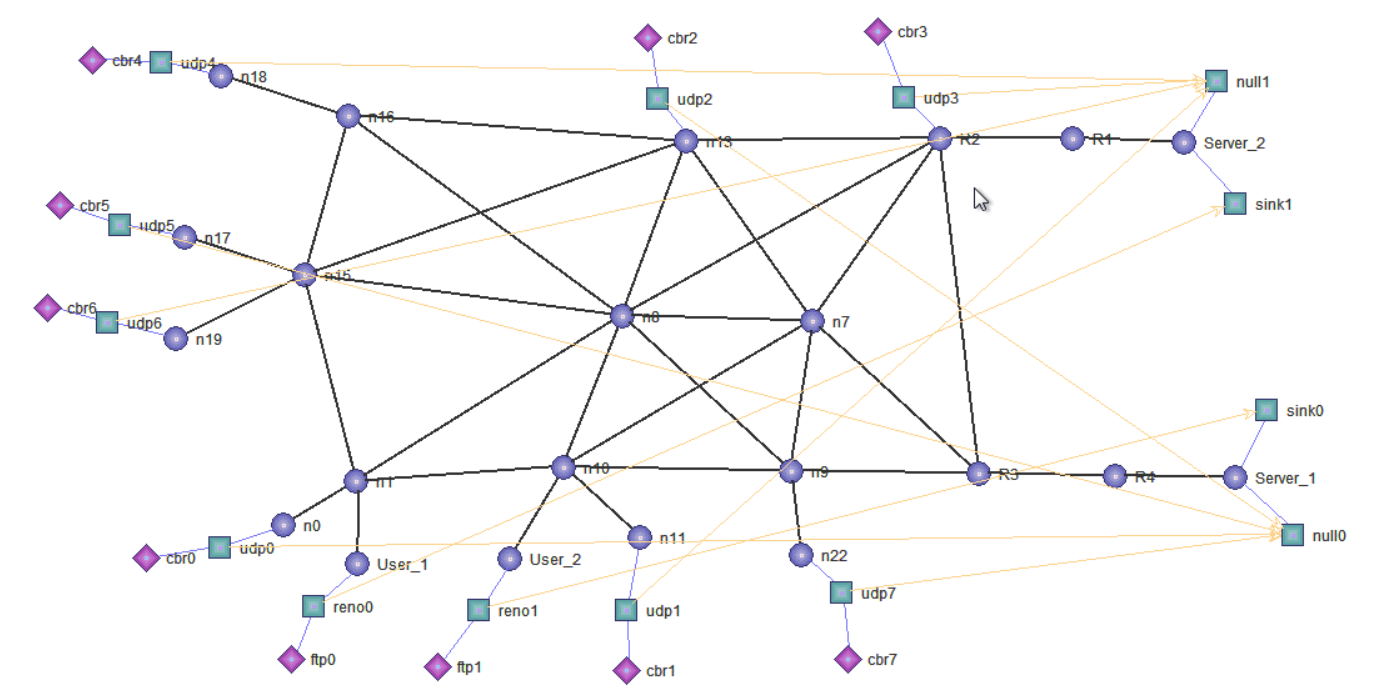
# PROJECT 3: DDoS Attack Simulation

**Network Architecture and Simulation Completion:**



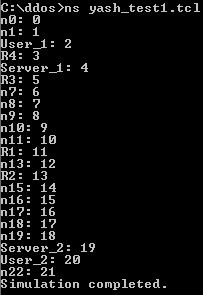


Table that captures the traffic that the attackers send out for the crossfire attack:

|  |  |  |
| --- | --- | --- |
| Source (attacker) | Destination | Traffic rate (KB per second) |
| CBR0 | Server 1 | 512 kb/s |
| CBR1 | Server 2 | 512 kb/s |
| CBR2 | Server 1 | 512 kb/s |
| CBR3 | Server 2 | 512 kb/s |
| CBR4 | Server 2 | 512 kb/s |
| CBR5 | Server 1 | 512 kb/s |
| CBR6 | Server 2 | 512 kb/s |
| CBR7 | Server 1 | 512 kb/s |
| TOTAL number of bots | 8 | Total traffic rate: 4096 kb/s |

# Below is a description of all the congested links and the packets being dropped because of the congestion in the nodes/links along with supporting screenshots from out.tr file: User 1- Server 2 Packet drop:

# The screenshot below from out.tr shows that the TCP packet which was meant for source user 1 and destination server 2 (node 2 and 19 respectively) was dropped between the links of node 13 and node 11. These links are R1 and R2, and the TCP packet drop occurred because of congestion generated by the CBR bots.



# User 2-Server 1 Packet Drop:

# The screenshot from out.tr below, shows the TCP Packet drop, which was originally meant for source User 2 and destination Server 1 (node 20 and node 4 respectively). The packet is dropped between the link of nodes 6 and 5 (The links are n7 and R3) and links of nodes 5 and 3 (The links are R3 and R4). This packet drop occurred because of the congestion caused by the CBR bots.

****

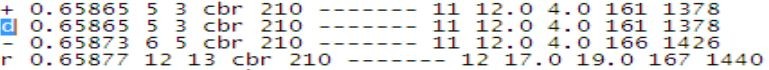
**Packet drops at congested links:**

**🡪Congestion between nodes R2 and R1:**

  
CBR and TCP packet drop between node 13 and node 11 i.e. links R2 and R1 because of congestion crossfire attack:

**🡪Congestion between nodes n7 and R3:**CBR and TCP packet drop between node 6 and node 5 i.e. links n7 and R3 because of congestion caused by crossfire attack:

# 🡪Congestion between nodes R3 and R4: CBR and TCP packet drop between node 5 and node 3 i.e. links R3 and R4 because of congestion caused by crossfire attack:



**What is a DDOS Attack?**

In a Distributed Denial of Service attack, an attacker tries to disrupt normal traffic flow of a targeted server/ service/network by overwhelming the target with more internet traffic than it can accommodate. The goal is to render the server/service/network, inoperable. DDOS attack is achieved by utilizing multiple compromised systems as a source of attack traffic.

**What is a crossfire attack?**

**Min Suk Kang, Soo Bum Lee CyLab and Virgil D** describe Crossfire attacks in their [paper](http://www.ieee-security.org/TC/SP2013/papers/4977a127.pdf) as: “a type of DDOS attack which aims to degrades and even cuts off network connections to a variety of selected server targets. This is achieved by simply ﬂooding only a few network links. In a Crossﬁre attack, a small set of bots directs low intensity ﬂows to a large number of publicly accessible servers. The concentration of these ﬂows on the small set of carefully chosen links ﬂoods these links and effectively disconnects selected target servers from the Internet. The sources of the Crossﬁre attack are undetectable by any targeted servers, since they no longer receive any messages, and by network routers, since they receive only low-intensity, individual ﬂows that are indistinguishable from legitimate ﬂows. The attack persistence can be extended virtually indeﬁnitely by changing the set of bots, publicly accessible servers, and target links while maintaining the same disconnection targets.”

**DDOS Attack Prevention Techniques:**

**🡪Ensuring extra bandwidth:** Overprovisioning bandwidth provides extra time to identify and deal with a DDoS attack.

🡪**Monitor the traffic:** DDoS attack causes huge abnormal traffic spike which could often be hidden amidst legitimate traffic. One should always monitor and look out for such abnormal traffic spike, even set up thresholds for automated report when traffic exceeds the baseline.

🡪**Use a CDN:** CDNs identify traffic launched as part of a DDoS attack & divert it to a third-party cloud infrastructure thus preventing DDOS. These are pretty expensive though.

🡪 **Purchase a dedicated server:** This will give you more bandwidth and greater control over security.

🡪Keep your system patched and updated.

🡪Train your users to be cyber secure and train them in incident handling and recovery

**Crossfire Attack Prevention Techniques:**

🡪With reference to this [IEE paper](https://ieeexplore.ieee.org/document/7796857), one can say that SDN can be leveraged to enable moving target defense (MTD) to mitigate Crossfire DDoS attack. The network states are continuously changed in MTD by effectively collecting information from the network and enforcing certain security measures on the fly in order to deceive the attackers. By relying on the ability of SDN and OpenFlow protocol and incorporating ICMP monitoring, traceroute profiling, route mutation and congestion-Link monitoring, this prevention measure takes place in two stages:

1. Obfuscating the links during the potential link-map creation of the attackers to make it harder to launch the attacks (i.e., proactive stage).
2. Detection and mitigation during the attacks (reactive stage).

🡪Another [paper](https://arxiv.org/abs/1812.03639) by [Akash Raj Narayanadoss](https://arxiv.org/search/cs?searchtype=author&query=Narayanadoss%2C+A+R), [Tram Truong-Huu](https://arxiv.org/search/cs?searchtype=author&query=Truong-Huu%2C+T), [Purnima Murali Mohan](https://arxiv.org/search/cs?searchtype=author&query=Mohan%2C+P+M), [Mohan Gurusamy](https://arxiv.org/search/cs?searchtype=author&query=Gurusamy%2C+M) suggests that SDNs dynamic network monitoring and traffic characteristic extraction capabilities can be utilized to develop a machine learning model which is capable of learning the temporal correlation among traffic flows traversing in the ITS network and thus, differentiate legitimate flows from coordinated attacking flows.

**References:**

<http://www.ieee-security.org/TC/SP2013/papers/4977a127.pdf>

<https://techspective.net/2017/05/11/20-ways-prevent-deadly-ddos-attack/>

<https://ieeexplore.ieee.org/document/7796857>

<https://arxiv.org/abs/1812.03639>