# PhD proposal
# SDN-based DDoS mitigation

Advisors: Abdelkader Lahmadi (Université de Lorraine, LORIA) / Romain Azaïs (INRIA, IECL), Isabelle Chrisment (Université de Lorraine, LORIA)

## Context

SDN (Software-Defined Networking) is a recent networking paradigm promoting high flexibility and configuration of networks. It allows to reconfigure forwarding devices (routers, switches). In such a context, SDN can be especially considered to get together network devices to counter-act against a running attack.

Distributed Denial-of-Service (DDoS) attacks represent a major threat in Internet [1,2] due to the disruption they cause and also the lack of an easy defense. These attacks launched from botnet or a collection of remotely-controlled computers to saturate data links leading to a target with hundreds of Gbps of traffic volume. Most of current techniques for mitigating DDoS attacks rely on increasing the service capacity by cloud-based techniques making thus the cloud absorbing the heavy load of the DDoS [3]. However, these solutions are costly and also introduce privacy issues since they require that companies redirect their network traffic to these cloud providers. In addition, many companies are not able to reroute their networks if they do not own their own IP range.

## Objective

The objective of the thesis is to design mechanisms to absorb attacks within the network itself. Indeed, the network devices represent available resources which can be used for absorbing the attacks, especially if all of them are well synchronized by empowering SDN and its capabilities of making dynamic and programmable networks.

The first research question to address is the orchestration of in-network absorption of large scale DDoS attacks, i.e. making the network a DDoS absorber. The goal is investigate how to use efficiently and as many as possible network paths as well as introducing delays in message delivery when a network is being attacked. However, due to the scale of some DDoS, we also investigate hybrid models. Hence, the second question is related to the synchronization of in-network and cloud-based absorption of DDoS.

## Approach

The thesis consists in selecting and adapting different mathematical techniques for modelling nodes interconnectivity as well as network traffic such that it is possible to redefine the associated traffic forwarding rules. The main challenge to address is scalability regarding the variety and number of traffic flows to handle and to mitigate DDoS attacks as fastest as possible. To achieve that, the PhD student will have to design new network management control mechanisms to proactively calculate undesired network states and their associated mitigation strategies. Then, based on network monitoring, the goal is to detect when the network changes (mainly traffic flows) tend to reach such an undesired situation and so trigger counter-measures (reconfiguration) at the right time. Therefore, a new orchestration technique leveraging SDN will be designed and evaluated, especially in terms of attack

mitigation efficiency (time to mitigate/recover to a normal state), network overhead (e.g. reconfiguration messages but also route instability if the system is too sensitive). As highlighted before, the resolution technique will also consider cloud services to deploy absorbing services, but they introduce an important cost that should be included in the traffic absorption model.

## References

[1] https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

[2] http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5351-arbor-networks-10th-annual-worldwide-infrastructure-security-report-finds-50x-increase-in-ddos-attack-size-in-past-decade

[3] Ping Du; Nakao, A., "DDoS defense as a network service," *Network Operations and Management Symposium (NOMS), 2010 IEEE* , vol., no., pp.894,897, 19-23 April 2010 doi: 10.1109/NOMS.2010.5488345