Bringing Private Traffic to Public SDN Testbeds

The combined efforts on exploring the possibilities of Software Defined Networking (SDN) for new network applications have led to the emergence of publicly accessible SDN testbeds all around the world. Examples include OFELIA and other FIRE-related activities, FIBRE, GENI, and JGN-X. However, these testbeds often run as stand-alone islands and have only limited possibilities to exchange traffic with the Internet for safety and privacy reasons. Safety considerations come into play when thinking about the damage, e.g., network outages, that can result from an experiment going bad. Moreover, an experimenter in an SDN testbed has a vast amount of control over the traffic, including the possibility to intercept, manipulate, and redirect communication. This immense power of the experimenter raises immediate privacy and availability concerns when thinking about having user traffic inside an SDN testbed. Nonetheless, experimenters would like to test out their inventions with user traffic for different reasons, e.g., investigating how a system performs under a real-world work load.

We are currently investigating how a compromise between the users' concerns and the experimenters' needs can be found. Ideally, an experimenter should be able to describe the type of traffic he needs for his experiment, and a user should be able to specify which parts of his traffic he is willing to make available under certain constraints. Such constraints could include keeping the traffic payload private, anonymizing endpoint addresses, or not passing some traffic through the testbed at all. Moreover, network availability should be guaranteed to the user whenever possible. This still leaves the question why users would be willing to share part of their traffic. However, building such a meeting point for experimenters and users allows to create a market place, where in addition to voluntarily donated traffic, experimenters can offer advantageous network features to users or even pay users in order to get access to the interesting parts of their traffic.

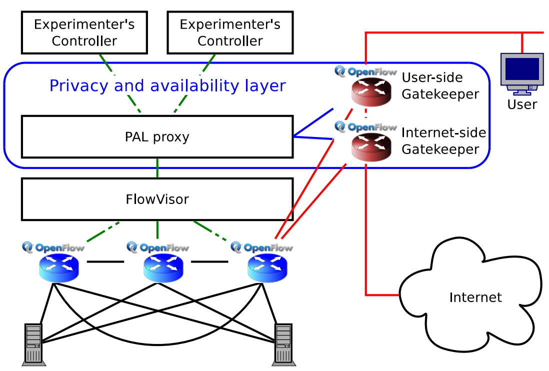
Prior work in constructing policing layers includes FlowVisor [5], VeriFlow [2], and Header Space Analysis (HSA) [1]. We build on HSA in order to enable injecting user traffic into a public testbed with privacy guarantees.

Tasks

We have implemented a prototype policing layer offering a "no-sniff" privacy guarantee [3]. The goal is to complete the functionality of this prototype for eventual deployment on our OFELIA [6] island. To achieve this, we have several implementation tasks open, including implementation of specific policies, an arbiter assigning user traffic to experiments, building a user web-interface for policy specification, and validation of the result.

Your work includes:

1. Studying related work on Software Defined Networking and OpenFlow.



Guaranteeing privacy in a testbed.

2. Implementing the arbiter assigning user traffic to experiments. This includes getting familiar with the Hassel library [1], the OpenFlow protocol [4], or a web development framework.
3. Validating and evaluating the resulting program within the OFELIA testbed.
4. Writing a project report.

Requirements

Good programming skills in Python, analytical thinking, creativity. This thesis offers practical and theoretical tasks, including the development of SDN controller software and validation tools.

Contact

Dr. Bernhard Ager, bager@tik.ee.ethz.ch, ETZ G 95
Vassilis Kotronis, vkotroni@tik.ee.ethz.ch, ETZ G 92

References

[1] Kazemian, P., Chang, M., Zeng, H., Varghese, G., McKeown, N., and Whyte, S. Real time network policy checking using header space analysis. In *Proc. of USENIX NSDI* (2013).

[2] Khurshid, A., Zou, X., Zhou, W., Caesar, M., and Godfrey, P. B. VeriFlow: verifying network-wide invariants in real time. In *Proc. of USENIX NSDI* (2013).

[3] Kotronis, V., Schatzmann, D., and Ager, B. On bringing private traffic into public sdn testbeds. In *ACM SIGCOMM HotSDN workshop* (2013). Poster abstract, to appear.

[4] ONF documents. https://www.opennetworking.org/about/onf-documents.

[5] Sherwood, R., Gibb, G., Yap, K.-k., Casado, M., McKeown, N., and Parulkar, G. Can the production network be the testbed. In *Proc. of USENIX OSDI* (2010).

[6] OFELIA. http://www.fp7-ofelia.eu/.

Preliminary time table

Task	Estimated duration
Familiarization with OpenFlow, Hassel, Mininet, OFELIA, existing code base	4 weeks
Designing the arbiter	2 weeks
Programming the arbiter and integration with PAL	8 weeks
Deployment inside OFELIA	1 weeks
Validation and evaluation	5 weeks
Writing the thesis	4 weeks
SUM	24 weeks