CleanSky ITN Summer School 2015
Abstract for Poster Presentation **Field of Study** Computer Sciences

Early-stage anomaly detection and mitigation in large-scale networks

Thien Xuan Phan and Kensuke Fukuda
National Institute of Informatics, JAPAN

Internet traffic anomalies cause a serious problem for the users and internet service providers (ISPs) since they degrade the availability of network services and prevent legitimate users from accessing the networks resources. Detecting and preventing the Internet traffic anomalies are crucial tasks to maintain the network services. Existing anomaly detection approaches are typically based on the conventional network architecture that demands heavy processing in order to extract feature information needed for traffic analysis. This disadvantage results in the rather large amount of delay time to detect anomalous traffic in case of network attacks, and thus the reaction against the attacks is rather inefficient. The mitigation of such anomalies in large-scale networks is even more challenging since a large number of switches/routers need to be investigated for such tasks in the networks.

This research topic aims to provide an efficient architectural solution for early-stage anomaly detection and mitigation of Internet traffic on large-scale networks. The key idea of this research is to propose a scalable network architecture that enables efficient query of network statistics, and an effective algorithm working on the network architecture to analyze the queried information for anomaly detection and suggest actions for mitigation of the attack traffic.