Background

Constantly changing and growing in number, the adversarial examples are hard to be collected completely and patterned, which makes it hardly possible to train the model of Intrusion Detection System (IDS) with sufficient patterns in the conventional sense, though it had been optimised by the Generative Adversarial Network (GAN). In this case, new approaches need to be proposed to deal with the problem of having to train the IDS model with limited examples.

Research Question

Can the machine, with the help of Robust Optimisation, be taught and trained to accurately identify the adversarial attacks that it has never met under the circumstance that the speed of the evolution of such attacks far exceeds that of collecting and patterning data?

Mingjian Tang, Shui Yu, University of Technology Sydney

A model based on the robust optimisation will be worked out to train IDS (with GAN) to more accurately identify the newly emerging adversarial attacks with limited examples instead of bunches of data, which improves the efficiency of the model training.

Mingjian Tang, Shui Yu, University of Technology Sydney

Key Word: Uncertainty sets

The working mechanism of robust optimisation (RO) to describe the uncertainty deterministically based on datasets (Neos n.d.). It was found that the RO methodology can successfully weaken the influence of small perturbations of the data on the feasibility properties of the usual solutions to real world LPs (Ben-Tal & Nemirovski, 2002). This research intends to ensure the validity of the training of the IDS (with GAN) with a limited size of examples, i.e., to reduce the uncertainty that limited samples bring about while achieving the same, or at least approximate, validity as in other cases with sufficient examples.

Mingjian Tang, Shui Yu, University of Technology Sydney

Distributionally Robust Optimisation (DRO)

DRO is a modelling framework significant both in the operations research and machine learning communities. It mainly deals with ambiguous stochastic optimisation problems. Assuming only partial distributional information, DRO models are closely connected to different concepts in statistical concepts, especially to robust optimisation. It has been viewed as a unifying framework for stochastic optimisation (SO) and robust optimisation (RO).

Mingjian Tang, Shui Yu, University of Technology Sydney