ABCData Webinar Series – CoDWeb - Complex Data Webinar, 9th April 2021

Detection of Internet Traffic Redirection Attacks using Symbolic Principal Component Analysis

M. Rosário Oliveira

CEMAT and Mathematics Department, Instituto Superior Técnico, Universidade de Lisboa

Internet security is a major concern for users and Internet Service Providers, since successful attacks can produce substantial damage. Illicit Internet traffic redirection cause man-in-the-middle attacks, in which a malicious agent secretly intercepts the traffic between two hosts connected to the Internet. The attack may be aimed at gaining access to sensitive information from the victim, monitoring its online activity, causing network delay, among other motivations.

To identify traffic redirection attacks we had access to measurements obtained from a worldwide distributed probing platform, designed to detect routing variations based on round-trip-times (RTT) deviations inferred from multiple and disperse geographic locations. The authors that conceived this infrastructure also developed an anomaly detection method based on average RTTs. Because these time measurements are inherently symbolic, we propose an alternative anomaly detection method based on histogram principal component analysis. To do so, we discuss how to define a linear combination of histogram-valued data and how to use the projected data on the first histogram principal component to successfully detect traffic redirections attacks. The effect of different choices for the symbolic covariance matrix and for the definition of histogram scores are also discussed.

This is a joint work with Ana Subtil, Eduardo Mendes, and Lina Oliveira.