Title: Identifying the Cyber Attack Origin with Partial Observation: A Linear Regression Based Approach

Speaker: Hamamache Kheddouci

Abstract: Cyber systems have become ubiquitous and indispensable in our daily life, and the extent of our dependence on them has increasingly grown in all fields including: education, business, industry and government. Those systems make intensive use of data and information and are therefore exposed to more potential cyber attacks. Thereby, the need for reliable approaches to protect them has increased. One of the key elements for guaranteeing the security of cyber systems is to identify the origin (the source) of the attack. In this paper, we describe a new approach to estimate both the source and the start time of a virus outbreak in complex networks (which include cyber systems) using partial information about the diffusion process, obtained through observing only a subset of nodes. Our approach uses a linear regression method on the partial obtained data, based on the fact that there is a linear correlation observed between the relative infection time of a node and its effective distance from the source. The experimental results showed that our approach is able to give an estimation of the source and the start time in, respectively, few hops from the actual source, and few time-units from the real start time.