Università degli Studi di Salerno
Dipartimento di Informatica

Dottorato di Ricerca in Informatica - X Ciclo

Tesi di Dottorato

Network Anomaly Detection Based On The Observation Of Multi-Scale Traffic Dynamics

Francesco Palmieri

Anno Accademico 2010-2011

Candidato:	Coordinatore:	Tutor:
Francesco Palmieri	Prof. Giuseppe Persiano	Prof. Alfredo De Santis

Abstract

With the rapid growth and the ever increasing complexity of the modern network infrastructures, the task of identifying and preventing network abuses is getting more and more strategic to ensure an adequate degree of protection from both external and internal menaces. In this scenario many techniques are emerging for inspecting the network traffic and modeling anomalous and normal behaviors to detect undesired or suspicious activities. First of all, the definition of normal or abnormal network behavior depends on several factors related to the day-to-day operations and resource usage. Normal behavior can only be determined by acquiring information about past events, but traffic trends usually take time to be understood and analyzed. This paradox can only be coped with by modeling the future behavior, based on a statistical idealization of the past events and an observation of the present ones and by specifically analyzing and observing some particularly discriminating statistical features and evolutive phenomena that occur on the network traffic. Since anomalous events are now conceived to be a structural part of the overall network traffic, it is more and more important to automatically detect, classify and identify them in order to react promptly and adequately. Accordingly the main focus of this dissertation is on developing a novel approach to network anomaly detection based on the analysis of complex non-stationary properties and "hidden" recurrence patterns occurring in the aggregated IP traffic flows. In the observation of the above transition patterns for detecting anomalous behaviors, we adopted several techniques that are known to be effective in exploring the hidden dynamics and time correlations of statistical time series, such as wavelet and recurrence quantification analysis. The resulting model, using supervised machine learning techniques to adaptively classify the traffic time series from the aforementioned observations, demonstrated to be effective for providing a deterministic interpretation of nonlinear patterns originated by the complex traffic dynamics observable during the occurrence of “noisy” network anomaly phenomena, characterized by measurable variations in the statistical properties of the traffic time series, and hence for developing qualitative and quantitative observations that can be reliably used in detecting such events.