SAMI 2020 Plenary Talk

Zsolt Csaba Johanyák: Fuzzy Logic based Network Intrusion Detection Systems

Abstract: Our everyday life is more and more dependent on electronic communication and network connectivity. However, the threats of attacks and different types of misuse increase exponentially with the expansion of computer networks. In order to alleviate the problem and to identify malicious activities as early as possible Network Intrusion Detection Systems (NIDSs) have been developed and intensively investigated. Several approaches have been proposed and applied so far for these systems.
It is a common challenge in this field that often there are no crisp boundaries between normal and abnormal network traffic, there are noisy or inaccurate data and therefore the investigated traffic could represent both attack and normal communication. Fuzzy logic based solutions could be advantageous owing to their capability to define membership levels in different classes and to do different operations with results ensuring reduced false positive and false negative classification compared to other approaches.
In this presentation, after a short introduction of NIDSs a survey will be done on typical fuzzy logic based solutions followed by a detailed description of a fuzzy rule interpolation based IDS. The whole development process, i.e. data preprocessing, feature extraction, rule base generation steps are covered as well.