

**CHENNAI – PONDICHERRY**

**ANOMALY DETECTION AND ATTRIBUTION IN NETWORKS WITH TEMPORALLY CORRELATED TRA**

**ABSTRACT:**

Anomaly detection in communication networks is the first step in the challenging task of securing a network, as anomalies may indicate suspicious behaviors, attacks, network malfunctions, or failures. In this paper, we address the problem of not only detecting the anomalous events but also of attributing the anomaly to the flows causing it. To this end, we develop a new statistical decision theoretic framework for temporally correlated traffic in networks via Markov chain modeling. We first formulate the optimal anomaly detection problem via the generalized likelihood ratio test (GLRT) for our composite model. This results in a combinatorial optimization problem which is prohibitively expensive. We then develop two low-complexity anomaly detection algorithms. The first is based on the cross entropy (CE) method, which detects anomalies as well as attributes anomalies to flows. The second algorithm performs anomaly detection via GLRT on the aggregated flows transformation - a compact low-dimensional representation of the raw traffic flows. The two algorithms complement each other and allow the network operator to first activate the flow aggregation algorithm in order to quickly detect anomalies in the system. Once an anomaly has been detected, the operator can further investigate which specific flows are anomalous by running the CE-based algorithm. We perform extensive performance evaluations and experiment our algorithms on synthetic and semi-synthetic data, as well as on real Internet traffic data obtained from the MAWI archive, and finally make recommendations regarding their usability.