Politecnico di Torino
SmartData@PoliTO

SmartData

June 19th, 2025, 5:00 PM CEST

SmartTalk: Covivio, Sala Grande

https://smartdata.polito.it/category/smarttalks/

Andrea Sordello

Andrea Sordello is a PhD student in Computer and Control Engineering at Politecnico di Torino, within the SmartData@PoliTO research center. His research focuses on network traffic analysis and the development of distributed platforms for cybersecurity.

What Erroneous Traffic Can Reveal: Unveiling Silent Anomalies from Passive Observations

ABSTRACT

Passive network measurement traditionally emphasizes inbound traffic for detecting threats and monitoring performance. **Outbound traffic generated by internal hosts** that fail to reach valid destinations or contains error messages remains largely unexplored.

We investigate the potential of such traffic to reveal **misconfiguration, internal faults, and malicious behaviour**. Leveraging a **SDN mechanism** explicitly designed to capture and log only **outbound erroneous traffic**, we present a characterization of this often overlooked data source.

Being a small fraction of overall traffic, explicitly focusing on the high signal-to-noise ratio of erroneous outbound packets is particularly valuable for detecting anomalies that may be obscured in bulk traffic flows. We demonstrate how simple analytics can uncover significant operational and relevant security events.