

Model Independent Probability Distribution Based Anomaly Detection Method

Disclosure Number

201303010

Technology Summary

The disclosure relates to a conference paper that was presented at the 11th International conference on Machine Learning and Applications in December of 2012. Intrusion detection is often described as having two main approaches: signature-based and anomaly-based. We argue that only unsupervised methods are suitable for detecting anomalies. However, there has been a tendency in the literature to conflate the notion of an anomaly with the notion of a malicious event. As a result, the methods used to discover anomalies have typically been ad hoc, making it nearly impossible to systematically compare between models or regulate the number of alerts. We propose a new, principled approach to anomaly detection that addresses the main shortcomings of ad hoc approaches. We provide both theoretical and cyber-specific examples to demonstrate the benefits of our more principled approach.

Inventor

FERRAGUT, ERIK M

Computational Sciences & Engineering Div

Licensing Contact

SIMS, DAVID L

UT-Battelle, LLC

Oak Ridge National Laboratory

Rm 124C, Bldg 4500N, MS: 6196

1 Bethel Valley Road

Oak Ridge, TN 37831

Office Phone: (865) 241-3808

E-mail: SIMSDL@ORNL.GOV

Note: The technology described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable. Patent applications directed towards this invention may not have been filed with any patent office.