

System for Anomaly Detection using Data-Driven Probabilistic Modeling

Disclosure Number

201102687

Technology Summary

With this technology, we propose a systematic method for constructing a potentially very large number of complementary anomaly detectors from a single probabilistic model of the data. This technology provides an automated method for learning the typical behavior of a cyber system, and then for using that typical behavior to automatically develop and implement a suite of anomaly detectors. The system provides real-time anomaly detection with (1) a collection of anomaly detectors rather than just one, (2) the ability to regulate false positive rates, and (3) context for each observed anomaly.

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.