# Edge Intrusion Detection with Distributed Novelty Detection: Design, Implementation and Evaluation

Luís Puhl, Hermes Senger, Guilherme Weigert Cassales
Universidade Federal de São Carlos, Brasil
Email: {luispuhl, gwcassales}@gmail.com, hermes@ufscar.br

***Abstract*—The implementation of the Internet of Things (IoT) is sharply increasing the small devices count and variety on edge networks and, following this increase the attack opportunities for hostile agents also increases, putting more pressure on the network administrator's need for tools to detect and react to those threats.**

**One such tool are the Intrusion Detection Systems (IDS) where the network traffic is captured and analysed raising alarms when a known attack pattern or new pattern is detected. To build an IDS one option for base algorithm are the Data Stream (DS) Novelty Detection (ND) being MINAS one of those.**

**Furthermore, for a network security tool to operate in the context of edge and IoT it has to comply with processing time, storage space and energy requirements alongside with traditional requirements for stream and network analysis like accuracy and scalability.**

**This paper addresses the construction details and evaluation of an prototype distributed IDS using MINAS ND algorithm. We discuss the algorithm steps, how it can be deployed in a distributed architecture, the impacts on the accuracy of MINAS and evaluate the performance and scalability using a cluster of constrained devices commonly found in IoT scenarios.**

**We found an increase of *0.0 y* processed network flow descriptors per core added to the cluster. Also *0.0 x1%* and *0.0 x2%* change in *F1Score* in the tested datasets when stream was unlimited in speed and limited to *0.0 z MB/s* respectively.**

***Index Terms*—novelty detection, intrusion detection, data streams, distributed system, edge computing, internet of things**

## I. Introduction

### Acknowledgment

The authors thank CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Código de Financiamento 001). Hermes Senger also thanks CNPQ (Contract 305032/2015-1) and FAPESP (Contract 2018/00452-2, and Contract 2015/24461-2) for their support.