

# IoT Intrusion Detection with Distributed Novelty Detection: Design, Implementation and Evaluation [DRAFT]

Luís Puhl, Guilherme Weigert Cassales, Hermes Senger, Helio Crestana Guardia  
Universidade Federal de São Carlos, Brasil  
Email: {luispuhl, gwcassales}@gmail.com, {hermes@, helio@dc.}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, requiring more from the network administrator role and the need for tools to detect and react to those threats. One such tool are the Network Intrusion Detection Systems (NIDS) where the network traffic is captured and analysed raising alarms when a known attack pattern or new pattern is detected. 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 traditional requirements for stream and network analysis like accuracy and scalability. This work addresses the construction details and evaluation of an prototype distributed IDS using MINAS Novelty Detection algorithm following up the previously defined IDSA-IoT architecture. We discuss the algorithm steps, how it can be deployed in a distributed environment, 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 *A* 0.0 processed network flow descriptors per core added to the cluster. Also *B* 0.0% and *C* 0.0% change in *FIScore* 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

The advent of Internet of Things (IoT) is growing the count and diversity of devices on edge networks, this growth increases network traffic patterns and extends opportunities for cyber attacks presenting new challenges for network administrators. To address those challenges new Network Intrusion Detection Systems (NIDS) and architectures can be explored, especially in Fog Computing and Data Stream (DS) areas.

Expected results: A system that embraces and explores the inherent distribution of fog computing in a IoT scenario opposing regular systems where data streams are collected and centralized before processing; Impact assessment of the impact of distributed, regional flow characteristics, local vs global vs distributed forgetting mechanism and other polices.

IDS characteristics and description of physical scenario.

MINAS characteristics.

Distribution and IDSA-IoT architecture.

This paper is structured as follows: Section II presents previous works that addresses related problems and how they influenced our solution. Section IV address our proposal, the work done, issues found during implementation and discusses parameters and configurations options and how we arrived at our choices. Section V shows experiments layouts and results, we compare serial and distributed implementation's metrics for validation, we also evaluate communication delay effects on classification metrics and conclude with the speedup per core and overall maximum stream speed. Section VI summarizes the research results and presents our final conclusions and future works.

## II. RELATED WORK

Recent works explored those areas, to name a few: BigFlow [1] employing Apache Kafka and Apache Flink for distributed stream processing evaluating with package stream dataset, CATRACA [2], [3] uses Apache Kafka and Apache Spark for stream processing and

## III. PROPOSAL

Fog computing infrastructure aims to offload computing resources from cloud providers by placing edge devices closer to end-users and/or data sources.

Objective: Distributed novelty detection in streams using limited hardware.

To achieve

## IV. IMPLEMENTATION

The original MINAS algorithm has a companion implementation (*Ref*) written in Java using MOA library base algorithms such as K-means and CluStream. *Ref* employs Java's double, a 64bits number whose precision is not absolutely necessary and, as it is often necessary to shuffle between nodes via network and a small economy could be made with only a float number with 32bits. Another difference between *Ref* and *MFOG* is cluster radius calculation from the distances of elements forming the cluster and the cluster's center, where the former uses the maximum distance, the latter uses the standard deviation of all distances as described in [4].

The stream format for input and output also of note. Input information needed is the value of the item, this value is a



TABLE I  
SERIAL IMPLEMENTATION: CONFUSION MATRIX AND QUALITATIVE METRICS

Classes (act) Labels (pred)	A	N	Assigned	Hits
-	16086	12481	—	0
0	94	3	A	94
1	995	94	A	995
10	34	0	A	34
2	104	0	A	104
4	0	47	N	47
5	23	0	A	23
6	3	0	A	3
7	29	0	A	29
8	46	11	A	46
N	429765	193642	N	193642
Metric	Value	Ratio		
Total input	653457			
Total output	653458			
Hits	195017	0.29843846		
Misses	429873	0.65784335		
Unknowns	28567	0.04371666		

implementation) and test set to compute a resulting output stream which is stored for qualitative evaluation using our python script evaluation. Therefore each experiment result consists of a time mesure (using GNU Time 1.9), qualitative overview mesure with the confusion matrix and qualitative stream measure with Stream hits and novelties visualization chart.

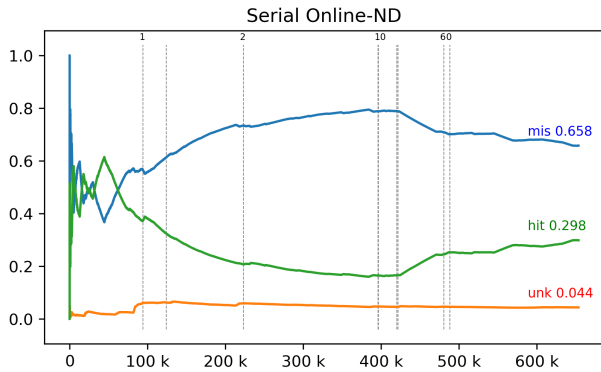


Fig. 3. Serial implementation: Stream hits and novelties visualization

	C N	C A
C N	181391 <sub>h</sub>	437837 <sub>m</sub>
N 1	0 <sub>m</sub>	123 <sub>h</sub>
N 2	13 <sub>m</sub>	35 <sub>h</sub>
N 3	0 <sub>m</sub>	6 <sub>h</sub>
N 4	43 <sub>m</sub>	483 <sub>h</sub>
N 5	0 <sub>m</sub>	52 <sub>h</sub>
N 6	0 <sub>m</sub>	164 <sub>h</sub>
N 7	314 <sub>h</sub>	2 <sub>m</sub>
N 8	97 <sub>m</sub>	939 <sub>h</sub>
N 9	826 <sub>m</sub>	2133 <sub>h</sub>
N 10	13887 <sub>h</sub>	3752 <sub>m</sub>
N 11	142 <sub>m</sub>	349 <sub>h</sub>
N 12	5793 <sub>h</sub>	1121 <sub>m</sub>
N 13	35 <sub>h</sub>	0 <sub>m</sub>
N 14	10 <sub>m</sub>	39 <sub>h</sub>
Unk	3727 <sub>u</sub>	144 <sub>u</sub>
Metric	Value	Ratio
Total output	653457	
Hits	205743	0.314853158
Misses	443843	0.679222963
Unknowns	3871	0.005923879
FNew	12.064786	
MNew	97.910904	
Err	70.811700	
Classes (act) Labels (pred)	A	N
-	3774 <sub>u</sub>	8206 <sub>u</sub>
1	123 <sub>h</sub>	0 <sub>m</sub>
10	2489 <sub>m</sub>	4066 <sub>h</sub>
11	71 <sub>m</sub>	289 <sub>h</sub>
12	26 <sub>h</sub>	0 <sub>m</sub>
2	145 <sub>h</sub>	79 <sub>m</sub>
3	368 <sub>h</sub>	44 <sub>m</sub>
4	8 <sub>h</sub>	0 <sub>m</sub>
5	52 <sub>h</sub>	0 <sub>m</sub>
6	165 <sub>h</sub>	0 <sub>m</sub>
7	1 <sub>m</sub>	229 <sub>h</sub>
8	1046 <sub>h</sub>	181 <sub>m</sub>
9	161 <sub>h</sub>	154 <sub>m</sub>
N	438750 <sub>m</sub>	193030 <sub>h</sub>
Metric	Value	Ratio
Total input	653457	
Total output	653457	
Hits	199708	0.30561766
Misses	441769	0.67604907
Unknowns	11980	0.01833326
Reprocessed	0	0.00000000

## VI. CONCLUSION

### ACKNOWLEDGMENT

The authors thank CNPq (Contract 167345/2018-4). Hermes Senger also thanks CNPq (Contract 305032/2015-1) and FAPESP (Contract 2018/00452-2, and Contract 2015/24461-2) for their support.

### REFERENCES

- [1] E. Viegas, A. Santin, A. Bessani, and N. Neves, "Bigflow: Real-time and reliable anomaly-based intrusion detection for high-speed networks," *Future Generation Computer Systems*, vol. 93, pp. 473 – 485, 2019. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167739X18307635>

- [2] M. E. Andreoni Lopez, "A monitoring and threat detection system using stream processing as a virtual function for big data," Theses, Sorbonne Université ; Universidade federal do Rio de Janeiro, Jun 2018. [Online]. Available: <https://tel.archives-ouvertes.fr/tel-02111017>
- [3] M. E. Andreoni Lopez, "A Monitoring and Threat Detection System Using Stream Processing as a Virtual Function for Big Data," Ph.D. dissertation, 2019.
- [4] E. R. d. Faria, A. C. Ponce de Leon Ferreira Carvalho, and J. Gama, "Minas: multiclass learning algorithm for novelty detection in data streams," *Data Mining and Knowledge Discovery*, vol. 30, no. 3, pp. 640–680, May 2015. [Online]. Available: <https://doi.org/10.1007/s10618-015-0433-y>
- [5] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," *Proceedings of the 1st Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2011*, pp. 29–36, 2011.
- [6] G. W. Cassales, H. Senger, E. R. DE FARIA, and A. Bifet, "IDSA-IoT: An Intrusion Detection System Architecture for IoT Networks," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, June 2019, pp. 1–7. [Online]. Available: <https://ieeexplore.ieee.org/document/8969609/>