Metrics for community dynamics applied to unsupervised attacks detection

Icube - Laboratoire des sciences de l'ingénieur,de l'informatique et de l'imagerie, UMR 7357
Université de Strasbourg, 67000 Strasbourg, France;

Laboratoire de Recherche de L'EPITA (LRE),
14-16 rue Voltaire, 94270 Le Kremlin-Bicètre, France

julien.michel@epita.fr

Directed by Pierre Parrend

Julien MICHEL
28/06/2023

Context

BIG DATA :

How to manage an ever increasing amount of data ?

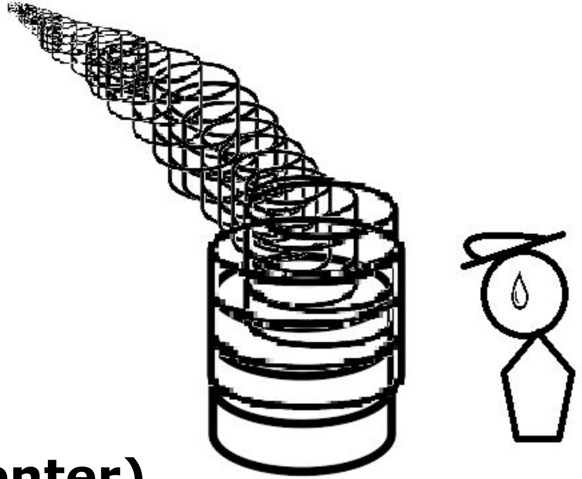
A.I.

?

A.I. CHALLENGES :

- Scalability
- Explainability
- Time robustness

Problem definition



DAMIAGE PROJECT

Core network Data

Continuous Data Stream

To help analyst in SOC (security operating center)

Constraints !!!

- New data have to be processed
- Data behaviours change with time

  = **Concept drift**
- Ever increasing amount of data

Unsupervised attacks detection

Principals characteristics :

- **Opposed to supervised approaches**
- **Do not make use of target label**

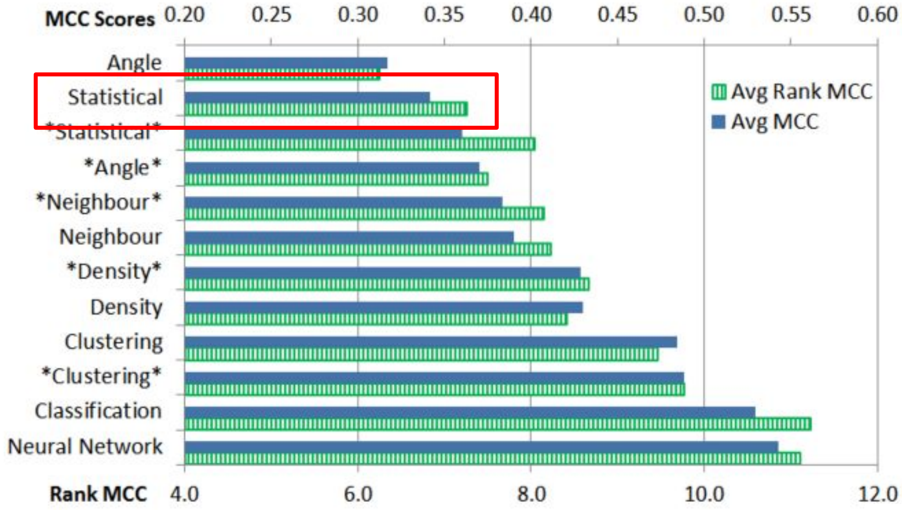
Why ?

At any time we may not have any prior knowledge to attacks we want to detect

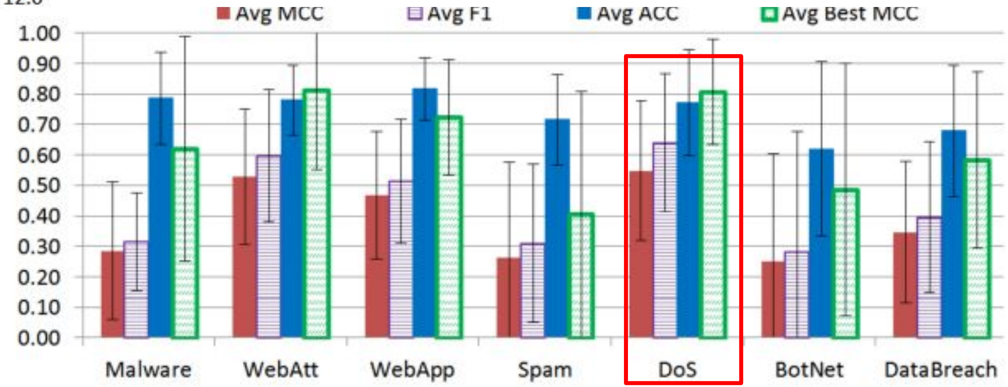
A new model is generated for any detection which may prove more secure

But important limits :

- Very sensitive to statistical anomalies
- Depending on the approach, it may prove hard to detect different types of attacks
- High false positive rate



#	Dataset	TNR Avg	P Avg	R Avg	F1 Avg	F1 Std	F2 Avg	ACC Avg	ACC Std	MCC Avg	MCC Std	Best MCC Avg	Best MCC Std
NF	Netflow-IDS	0.892	0.72	0.93	0.74	0.24	0.80	0.90	0.06	0.75	0.26	0.89	0.20
AM	AndMal17	0.665	0.23	0.37	0.18	0.05	0.24	0.62	0.06	0.05	0.63	0.10	0.04
C7	CICIDS17	0.647	0.47	0.72	0.47	0.29	0.53	0.68	0.19	0.37	0.23	0.70	0.38
C8	CICIDS18	0.806	0.75	0.76	0.67	0.18	0.71	0.73	0.19	0.59	0.32	0.84	0.23
CI	CIDDS	0.601	0.42	0.77	0.43	0.34	0.49	0.63	0.33	0.36	0.48	0.56	0.36
CT	CTU13	0.752	0.03	0.33	0.03	0.00	0.05	0.75	0.00	0.04	0.16	0.25	0.00
IX	ISCX12	0.778	0.66	0.78	0.63	0.36	0.65	0.80	0.15	0.56	0.17	0.86	0.16
NG	NGDIS	0.796	0.40	0.65	0.39	0.13	0.45	0.79	0.07	0.38	0.26	0.86	0.15
NK	NSLKDD	0.875	0.52	0.55	0.44	0.17	0.46	0.86	0.10	0.41	0.53	0.66	0.07
UG	UGR16	0.699	0.44	0.65	0.37	0.29	0.39	0.67	0.23	0.33	0.29	0.51	0.28
UN	UNSW	0.853	0.73	0.56	0.55	0.16	0.54	0.80	0.13	0.47	0.36	0.70	0.12



State of Art

Our approach is able to obtain 0.91 average MCC for Dos and Scan attacks in the UGR16 dataset with Isolation forest

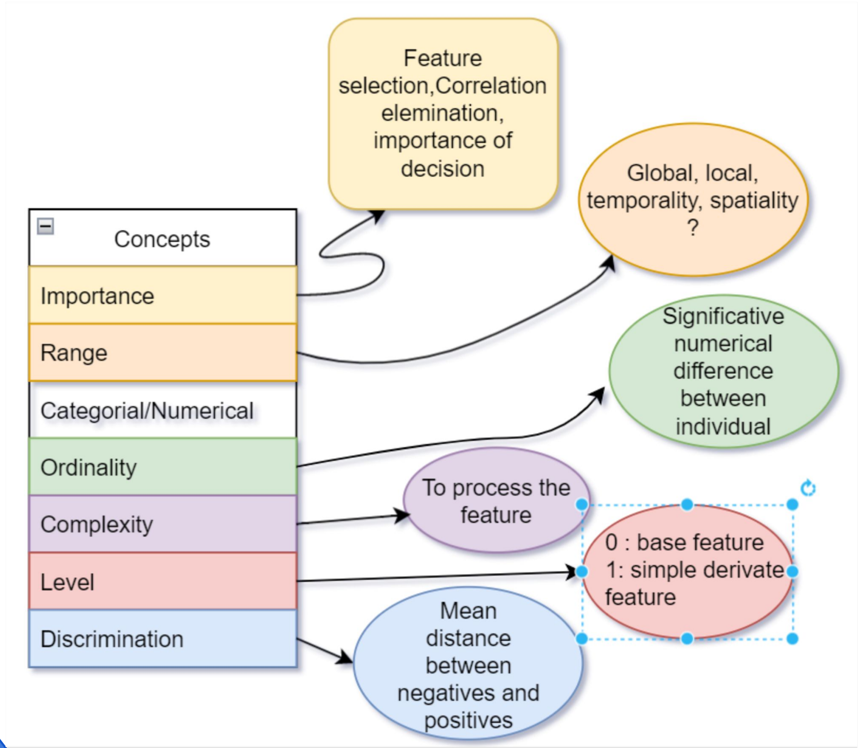
Tommaso Zoppi, Andrea Ceccarelli, Tommaso Capecchi, and Andrea Bondavalli. 2021. Unsupervised Anomaly Detectors to Detect Intrusions in the Current Threat Landscape

UGR'16 Dataset

Date time	Duration	Source IP	Destination IP	Source Port	Destination Port	Protocol	Flag	Forwarding status	ToS	Packets	Bytes	Label
2016-07-27 13:43:29	0.0	143.72.8.137	42.219.158.161	53	43192	UDP	.A....	0	0	1	214	background
2016-07-27 13:43:29	0.0	42.219.154.119	143.72.8.137	60185	53	UDP	.A....	0	0	1	72	background
2016-07-27 13:43:30	0.0	42.219.154.107	143.72.8.137	48598	53	UDP	.A....	0	0	1	77	background
2016-07-27 13:43:30	0.0	42.219.154.98	143.72.8.137	51465	53	UDP	.A....	0	0	1	63	background
2016-07-27 13:43:30	0.0	43.164.49.177	42.219.155.26	80	37934	TCP	.A...F	0	0	1	52	background

- Background data gathered from march to august 2016
- Simulated attacks from the last week of july and august in the background data. (DoS and Port Scan)
- Re-inserted some attacks detected using anomaly detection . (Spam and Botnet)
- Some unnoticed attacks may still be labelled as background

Why Graph community metrics ?



- Features are an important aspect if not the most important in anomalies detection.
- You need to keep only relevant features
- They need to discriminate positive and negative
- They need to be computable in your study case

Why Graph community metrics ?

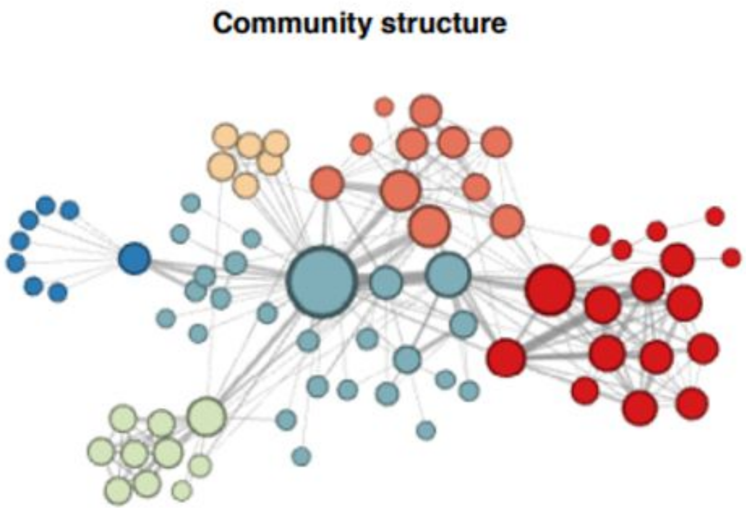
Unsupervised detection algorithms need to be fed the right features and only the right features !!!

How do you make attacks different from normal data ?

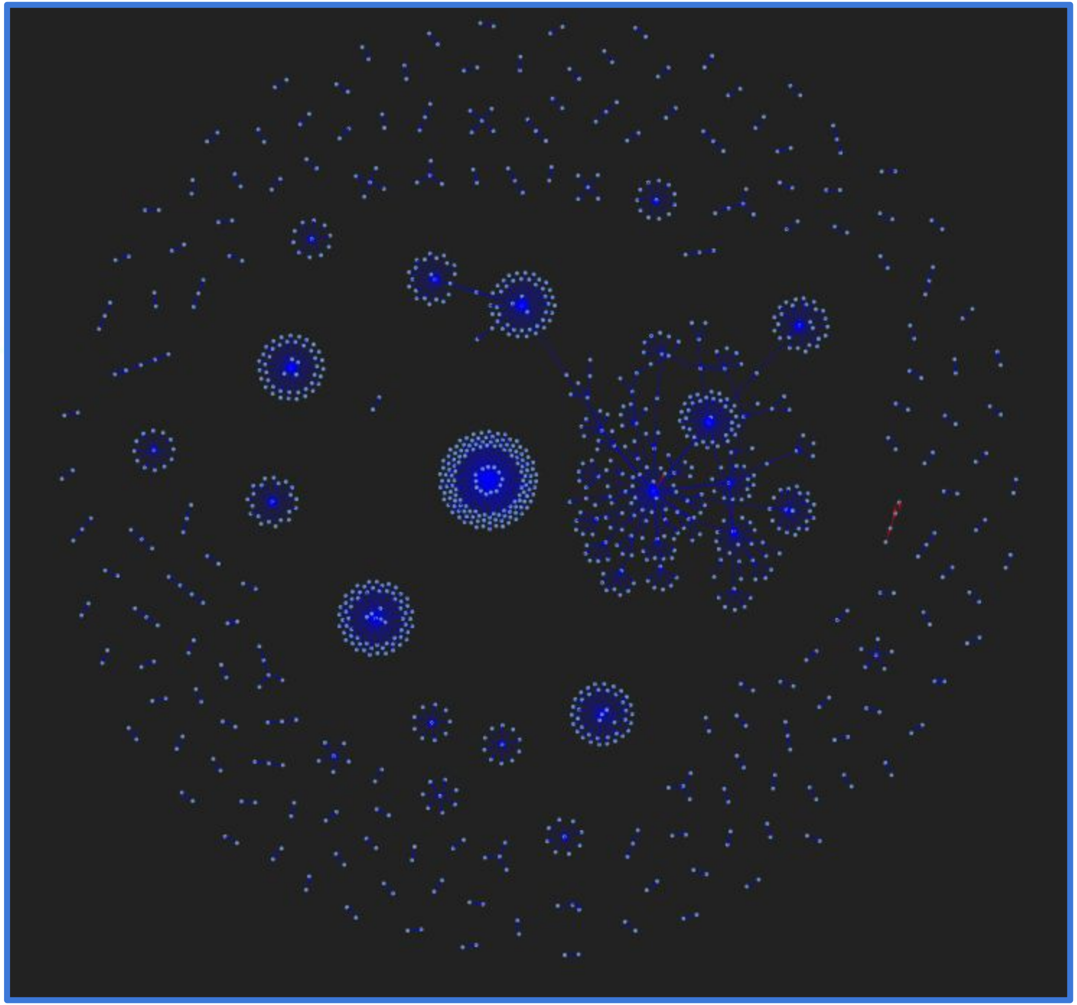
Graph representation is commonly used for network data
→ Topological informations

Attacks will have an impact on part of the topology of the network
→ part of the graph are the community

=> graph community metrics can be used as indicators

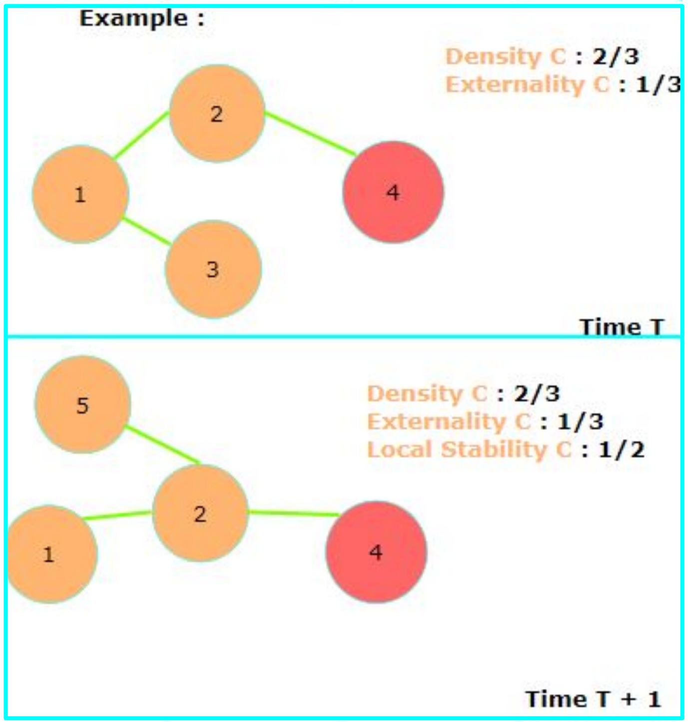


Static graph of a small sized sample of UGR'16 (~ 1000 edges)



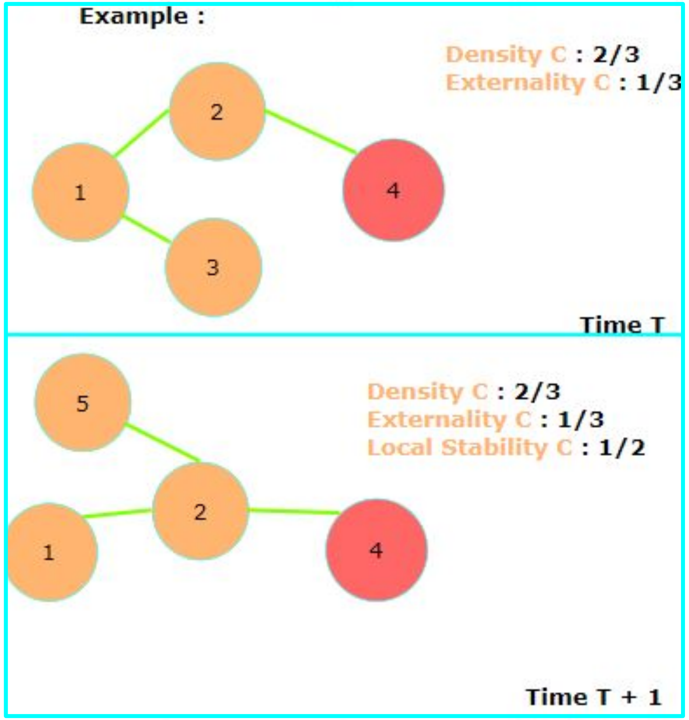
- For a **community C1** inside a graph G1 at time T and a **community C1'** inside a graph G2 at time T+1, the following metrics have been considered:

- **Density** : Number of connexion (a connexion being the existence of at least one edges between two nodes) with both nodes inside C1 divided on the maximal possible connexions inside C1.
- **Externality** : Proportion of edges with a source belonging to C1 and with a destination inside G1 but which doesn't belong to C1.



- A way to define the proportion of change in a community between two times of a dynamic graph has been introduced as the **local graph stability** .

- **Local Stability** : Proportion of similarity between C1 and C1', C1 and C1' being the same community at following times.
- **Global Stability** : Mean of all the local stabilities of a community .



METRICS	Selected	Useful (a priori)	Types of graph	Intervals
Density			IP, (IP,Port)	5,10** & 20 min
Externality			(IP,Port)	5 min
Local Stability			IP	20 min
Global Stability				
Coverage				
Modularity				
Isolability				
Unifiability				
Mean size			(IP,Port)	5 min

List of community metrics calculated for different types of graph on different time intervals for dynamic graph construction

Date time	Duration	Source IP	Destination IP	Source Port	Destination Port	Protocol	Flag	Forwarding status	ToS	Packets	Bytes	Label
2016-07-27 13:43:29	0.0	143.72.8.137	42.219.158.161	53	43192	UDP	.A....	0	0	1	214	background
2016-07-27 13:43:29	0.0	42.219.154.119	143.72.8.137	60185	53	UDP	.A....	0	0	1	72	background
2016-07-27 13:43:30	0.0	42.219.154.107	143.72.8.137	48598	53	UDP	.A....	0	0	1	77	background
2016-07-27 13:43:30	0.0	42.219.154.98	143.72.8.137	51465	53	UDP	.A....	0	0	1	63	background
2016-07-27 13:43:30	0.0	43.164.49.177	42.219.155.26	80	37934	TCP	.A...F	0	0	1	52	background

Only Those Column are used for the graph metrics based detection model.

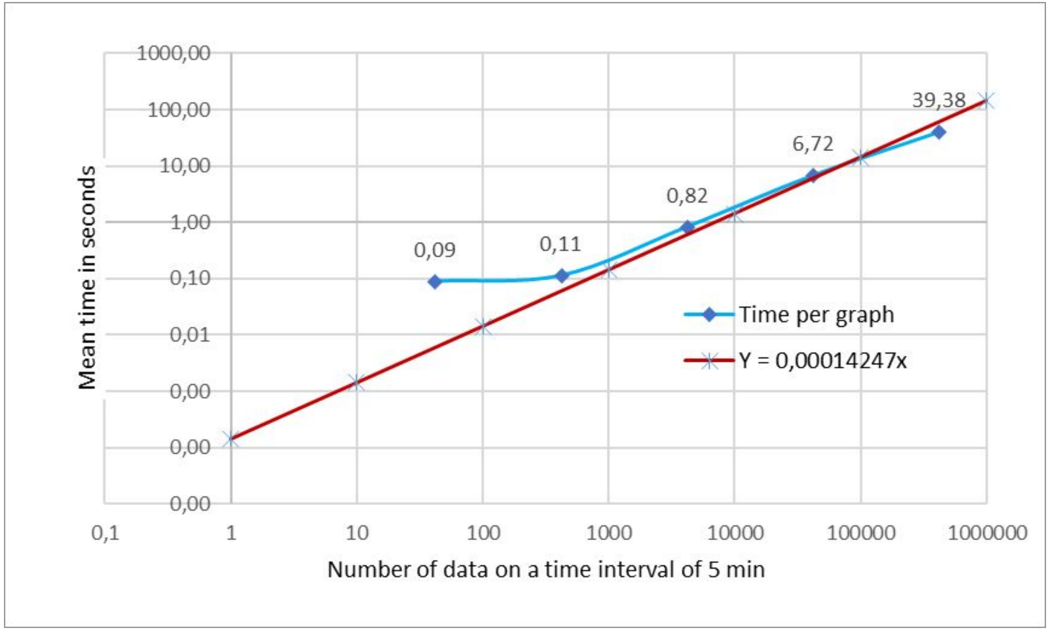
	F-score	MCC	Balanced Accuracy	AUPRC	Accuracy	Precision	Recall
Louvain	**0,825496**	**0,825035**	**0,936672**	**0,829467**	**0,996309**	**0,875822**	**0,780659**
LPA	0,75466	0,753257	0,898229	0,758666	0,994788	0,799695	0,714434

Community extraction algorithms

	F-Score	MCC	Balanced Acc	AUPRC	Acc	Precision	Recall
After sampling	0,502533	0,541945	**0,906327**	0,594621	0,991991	**0,81981**	0,362313
Before sampling	**0,679035**	**0,676763**	0,858336	**0,683339**	**0,993179**	0,720738	**0,641914**

Impact of sampling on detection performance

Scalability evaluation



3 algorithms have been set up for extraction of graph community metric in time which scale linearly

Attack patterns

- Approach used in real world security operations center
- 1 pattern => 1 type of attack
- 1 type of attack => n patterns
- Pattern deducted from characteristics of attacks in the literature

=> Can be used a baseline for our approach

Attack	Type	Criteria	UGR-16
DoS	Service overload	Port number = CONSTANT and number of message between Ip source and destination spaced by less than 3 min over : **[total_number_of_flow*0.0002* sampling]**	True Port = 80
Scan	Port scan	Number of messages between Ip source and destination spaced by less than 3 min over : **[total_number_of_flow*0.0002* sampling]** and number of different ports between the two ip over 50	True

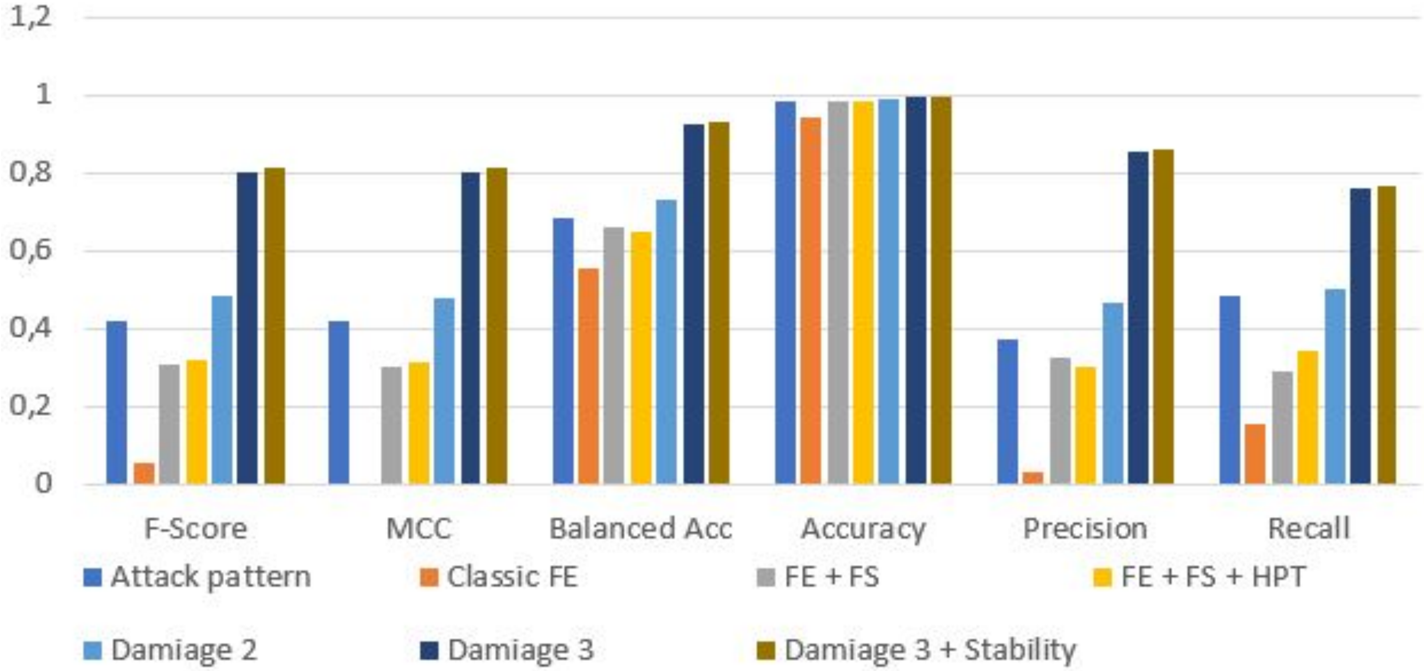
Scan False Positive Rate : 0.00116809518 / DoS FPR : 0.00227426215

Scan True Positive Rate : **0.68578661065** / DoS TPR : **0.2593768905**

Scan False Negative Rate : **0.30333205668** / DoS FNR : **0.7406231095**

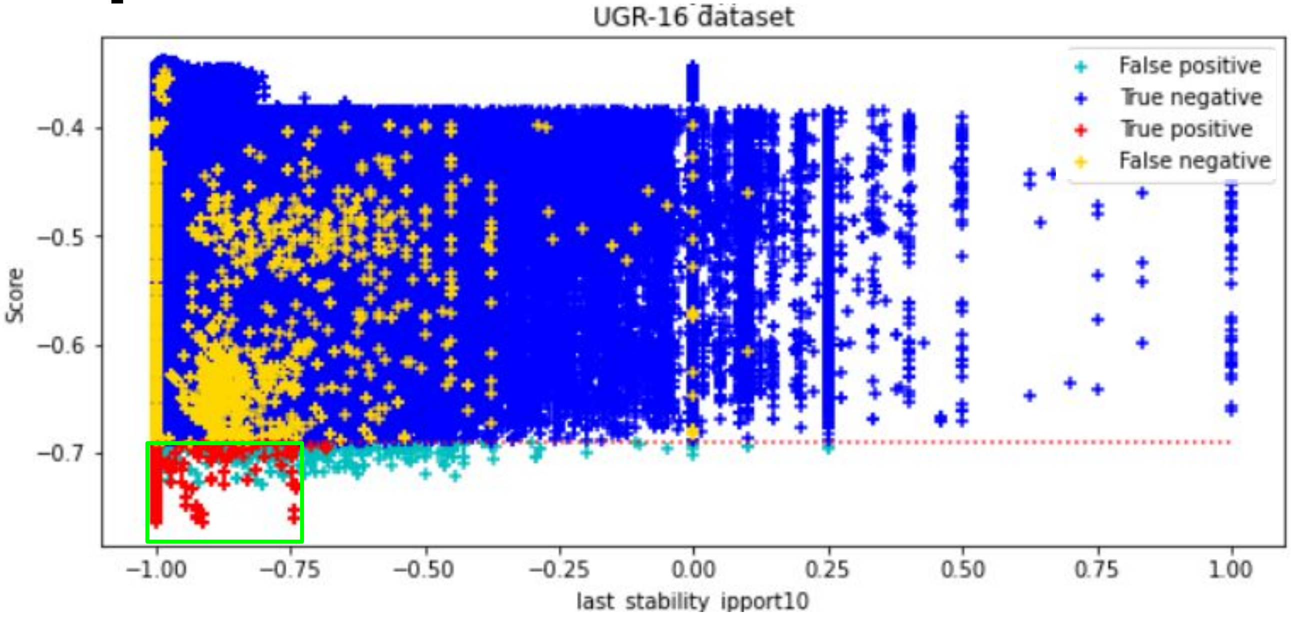
Scan True Negative Rate : 0.9988912 / DoS TNR : 0.99772573785

Results



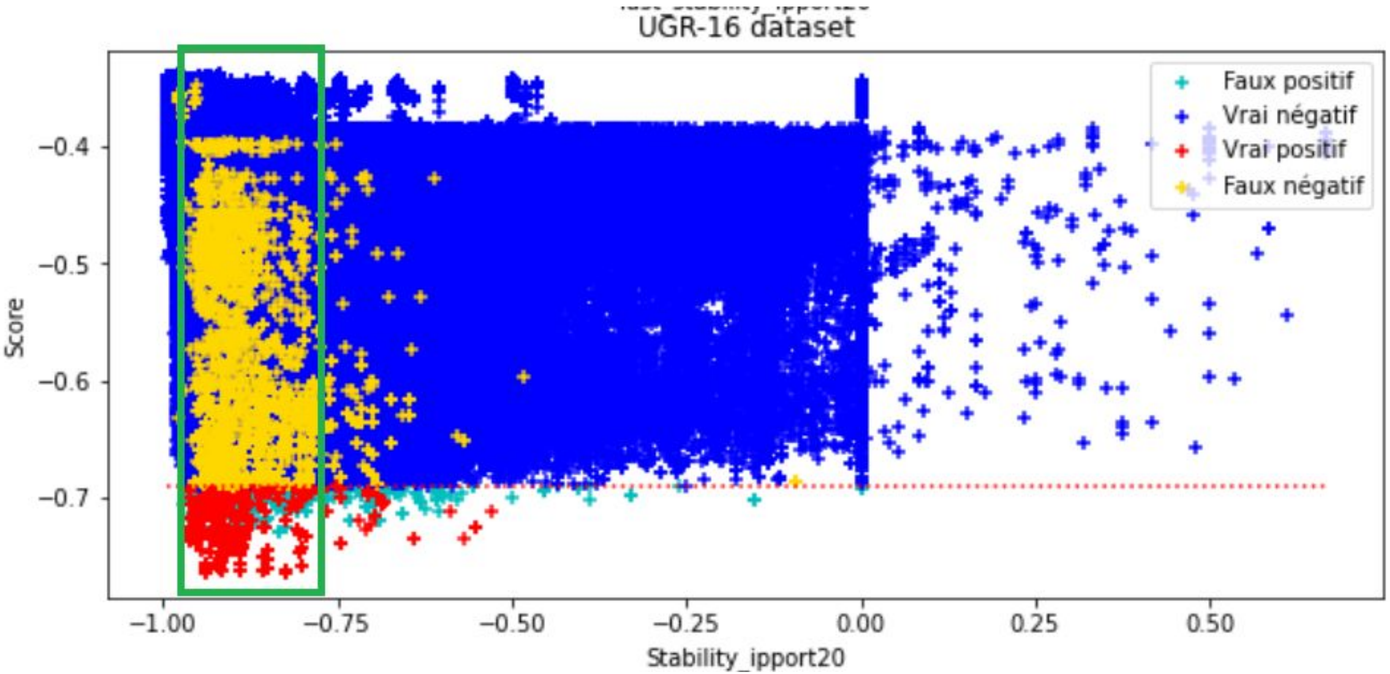
Detection score depending on the method using isolation forest algorithm on the same sample of data of the UGR'16 dataset

False positive reduction



Precision 87.84 % before false positive reduction and 89.38% after reduction.
=> 12.68% of false positives can be avoided.

False negative reduction ?



Actually, while 80% of the false negatives are in the Green zone, they only represent 0.31% of the negatives in this zone.

Conclusions

Feature extraction and selection are very important !

Graph community metrics seems relevant to the detection of cyber attacks

It is especially true for unsupervised detection !

An approach which fulfill the constraint of scalability and time robustness has been set up !

But, there are still a significant amount of false positive and the approach has only shown results on 2 types of attacks.

Next steps

- Application of the approach to data stream
- Define a pipeline and approach to tackle concept drift
- Find more robust and more specific to attacks behaviour features.

Icube - Laboratoire des sciences de l'ingénieur,de l'informatique et de l'imagerie, UMR 7357
Université de Strasbourg, 67000 Strasbourg, France;

Laboratoire de Recherche de L'EPITA (LRE),
14-16 rue Voltaire, 94270 Le Kremlin-Bicètre, France

julien.michel2@etu.unistra.fr

Thank you

[1] A. Abou Rida, R. Amhaz, and P. Parrend. Anomaly Detection on Static and Dynamic Graphs using Graph Convolutional Neural Networks, chapter -, page 23. Studies in Computational Intelligence Series. Springer, 2022.
[2] Siddharth Bhatia, Bryan Hooi, Minji Yoon, Kijung Shin, and Christos Faloutsos. Midas : Microclusterbased detector of anomalies in edge streams. In Proceedings of the AAAI Conference on Artificial Intelligence, volume 34, pages 3242–3249, 2020.
[3] Xavier Larriva-Novo, Víctor A. Villagrá, Mario VegaBarbas, Diego Rivera, and Mario Sanz Rodrigo. An iot-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors, 21(2), 2021.
[4] Gabriel Maciá-Fernández, José Camacho, Roberto Magán-Carrión, Pedro García-Teodoro, and Roberto Therón. Ugr‘16 : A new dataset for the evaluation of cyclostationarity-based network idss. Computers & Security, 73 :411–424, 2018.
[5] J. Navarro, A. Deruyver, and P. Parrend. A systematic survey on multi-step attack detection. Computers and Security, page 102, 2018.
[6] William Robertson, Giovanni Vigna, Christopher Krügel, and Richard Kemmerer. Using generalization and characterization techniques in the anomaly-based detection of web attacks. In NDSS, 01 2006.
[7] Jaewon Yang and Jure Leskovec. Defining and evaluating network communities based on ground-truth. In Proceedings of the ACM SIGKDD Workshop on Mining Data Semantics, MDS ’12, New York, NY, USA, 2012. Association for Computing Machinery.
[8] Tommaso Zoppi, Andrea Ceccarelli, Tommaso Capecchi, and Andrea Bondavalli. Unsupervised anomaly detectors to detect intrusions in the current threat landscape. ACM/IMS Trans. Data Sci., 2(2), apr 2021