AI & Networks

09:00-17:00, January 28

Predictive Network Maintenance

Speakers:
Imen Grida Ben Yahia (Orange) and Yoichi Matsuo(NTT)

NTT

orange™

Predictive Network Maintenance

- ❑ Definition and Motivation
- ❑ Orange and NTT activities
- ❑ Some ML strategies
- ❑ Zoom on Syslog analysis
- ❑ Zoom on Root cause analysis
- ❑ Take-away messages

Predictive Network Maintenance: Definition and motivation

Why	What
❑ Maintain service quality and availability	❑ detection and prediction of network and service events (failure, changes, degradations, etc.),
❑ Meet customer expectations	❑ diagnosis and root cause analysis
❑ Control and anticipate end to end networks when abnormal event occurs	❑ Recommendation of mitigation actions after failure

Predictive Network Maintenance: Some Orange activities

Decision making

Joint QoS and Energy Consumption control in RAN

Surrogate Based Centralized Self-Optimization

Intervention filtering for DSL or FTTH

SON conflict resolution

Cognitive SON management

Decision support

FTTH fault diagnosis

SON conflict diagnosis

Anticipation of SLA violations

Self-modelling based diagnosis for SDN

Knowledge creation

Fault detection in RAN

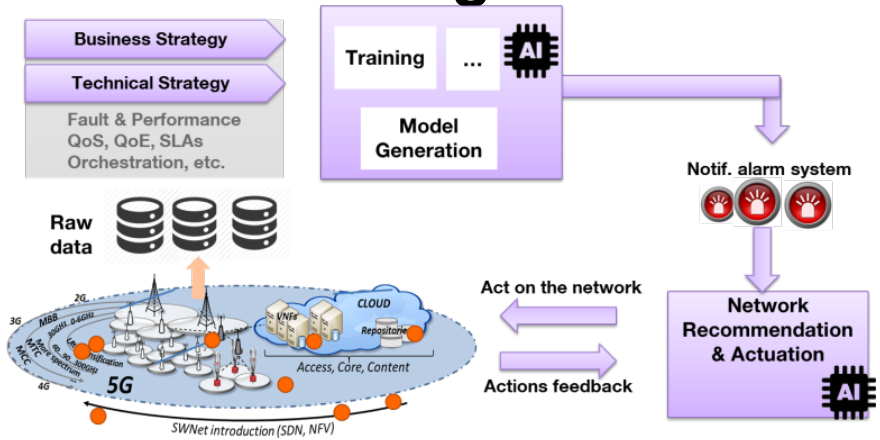
Black box anomaly detection in virtual networks

Customer QoS determination on living places

Best configuration for best results

Resource consumption attack detection in IaaS cloud

Large scale event prediction



Network data

Software network data

network and external data

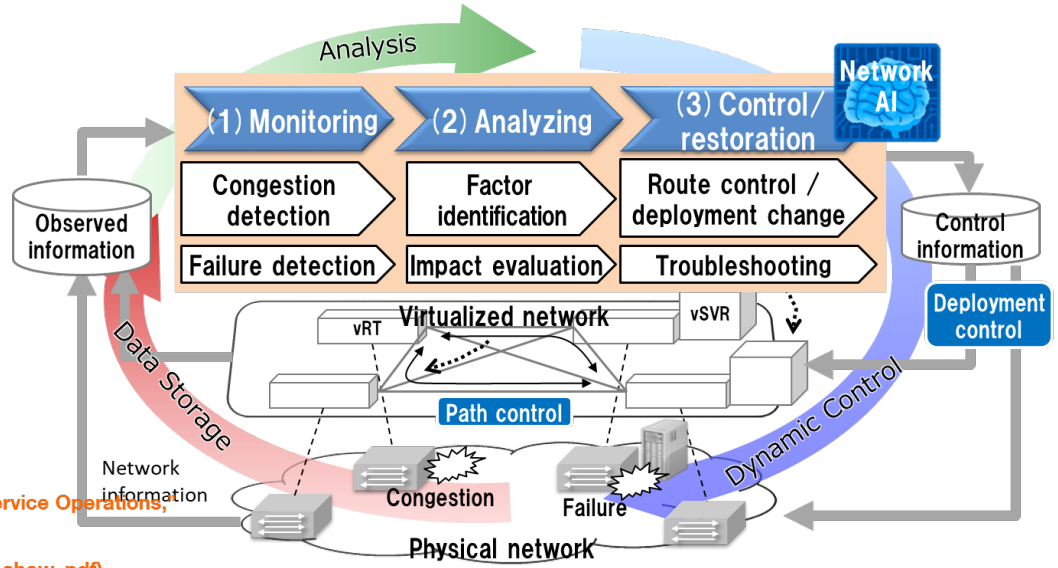
Predictive Network Maintenance: NTT activities

Motivation: In coming 5 years, 30-40% of our employees will be retiring. Replace skilled engineers' work with machine work.

Goal: Operational processes and tasks (such as delivery, deployment, configuration, assurance, and optimization) executed automatically, ideally with 100% automation.

We are developing "Proactive Controlled Network concept" ([1])

(1) Monitoring: Detection of NW state change (failure, congestion, etc.)
(2) Analyzing: Identification of degradation factors, failed equipment
(3) Control: Avoiding performance degradation and early restoration



[1] Keishiro W., at el., "Creating New Value by Leveraging Network-AI Technology in Service Operations," NTT Technical Review, vol.16, no.6, Jun. 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201806fa3.pdf&mode=show_pdf)

Predictive Network Maintenance: Some strategies from ML perspective

(Proactive) Regression ML models to predict the remaining useful lifetime (RUL)

(Reactive) Unsupervised detection of anomalous behavior

(Reactive) Causal model/classification for Root cause analysis

(Proactive or Reactive) Classification models to predict failure within a given time window

Etc.

Predictive Network Maintenance: Some strategies from ML perspective

1. (Proactive) Regression ML models to predict the remaining useful lifetime (RUL)

Input data: Static and historical network data and the degradation is incremental
Labeling: Every network event is labeled. Several events of each type of failure are present in the dataset
Output: Prediction of the RUL which is the time left for a network entity to be in a failure status, that could be in days, miles or cycles, etc.
Models: ML or DL regression models

2. (Proactive & Reactive) Classification models to predict failure within a given time window

Input data: Static and historical network data, failure type classes (e.g. based on historical alarm data)
Labeling: data are labeled and each class cases corresponding to a failure are representative within the data set. The failure is defined in a time window
Output: will be in the form of set of classes : class: A, Class: B etc. e.g. the PCRF will be down in the time window [x,y].
Models: *decision trees, SVM, deep learning, logistic regression.*

Predictive Network Maintenance: Some strategies from ML perspective

3. (Reactive) Unsupervised detection of anomalous behavior

Input data: Time-series data (traffic volume, CPU usage, etc.), Text data (syslogs), Categorical data (IP address, etc.)
Labeling: Half labeled (Only data in normal status exist), or no label at all
Output: RMSE of the test data, which shows degree of abnormality
Models: Multimodal VAE, AE.
Unsupervised approaches are better for anomaly detection due to lack of abnormal data

4. (Reactive) Causal model/classification for Root cause analysis: Identifying failed equipment, degradation factors

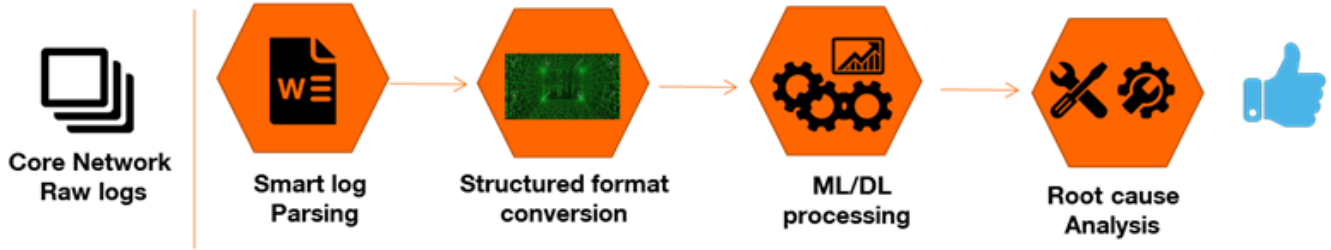
Input data: Time-series data (traffic volume, CPU usage, etc.), Text data (syslogs),
Labeling: Failure events data exist
Output: Estimated failed equipment or causes
Models: Bayesian Network, Supervised approach (Classification model). By learning the relationship between the failure events and input data using past failure events dataset, models localize root cause for test input data

Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
--Motivation & high level view

Motivation

- ❑ Network equipment system logs record important network events
- ❑ Log records are very useful to detect abnormal NE behavior
- ❑ Log records enable the Root Cause Analysis

High level log mining pipeline



Predictive Network Maintenance: *Zoom on Anomaly detection for logs* -- NetLogParser panorama

Active research field

Log Parser	Year	Technique	Mode	Efficiency	Coverage	Preprocessing	Open Source	Industrial Use
SLCT	2003	Frequent pattern mining	Offline	High	✗	✗	✓	✗
AEL	2008	Heuristics	Offline	High	✓	✓	✗	✓
IPLoM	2012	Iterative partitioning	Offline	High	✓	✗	✗	✗
LKE	2009	Clustering	Offline	Low	✓	✓	✗	✓
LFA	2010	Frequent pattern mining	Offline	High	✓	✗	✗	✗
LogSig	2011	Clustering	Offline	Medium	✓	✗	✗	✗
SHISO	2013	Clustering	Online	High	✓	✗	✗	✗
LogCluster	2015	Frequent pattern mining	Offline	High	✗	✗	✓	✓
LenMa	2016	Clustering	Online	Medium	✓	✗	✓	✗
LogMine	2016	Clustering	Offline	Medium	✓	✓	✗	✓
Spell	2016	Longest common subsequence	Online	High	✓	✗	✗	✗
Drain	2017	Parsing tree	Online	High	✓	✓	✓	✗
MoLFI	2018	Evolutionary algorithms	Offline	Low	✓	✓	✓	✗

[ICSE'19] Jieming Zhu, Shilin He, Jinyang Liu, Pinjia He, Qi Xie, Zibin Zheng, Michael R. Lyu. Tools and Benchmarks for Automated Log Parsing. *International Conference on Software Engineering (ICSE)*, 2019.

Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
-- NetLogParser panorama

E.g. Frequent Pattern Mining

1) traversing over the log data by several passes,

2) building frequent item sets (e.g., tokens, token-position pairs) at each traversal,

3) grouping log messages into several clusters,

and 4) extracting event templates from each cluster.

Example of log parsers ouputs

Spell	[ICDM'16] Spell: Streaming Parsing of System Event Logs, by Min Du, Feifei Li.

log message (log key underlined)	log key	parameter value vector
t_2 Took 0.61 seconds to deallocate network …	k_2 (id:2)	$[t_2 - t_1, 0.61]$
t_3 VM Stopped (Lifecycle Event)	k_3 (id:3)	$[t_3 - t_2]$
…	…	…

LogCluster	[CNSM'15] LogCluster - A Data Clustering and Pattern Mining Algorithm for Event Logs, by Risto Vaarandi, Mauno Pihelgas.

- Jan 1 *{4,4} (j+0KUw==) CMD (newsyslog)
  - Support : 1,500
- Dec 31 *{4,4} (j+0KUw==) CMD (newsyslog)
  - Support : 8,100
- Jan 1 *{1,1} LJBY+E2OYE6Lrtrm LJBY+E2OYE6Lrtrm ksyncd[21093]: ksyncd_ksync_handle_asyncmsg: *{4,4}
  - Support : 14,832
- Jan 1 *{1,1} AKNJX4pZZrSun5oOvHsjw/qJ0A== war_epc_kaz2_re1 ksyncd[3819]: ksyncd_ksync_handle_asyncmsg: *{4,4}
  - Support : 31,181
- Jan 1 *{1,1} Qe3DMJj74WvYeA19lNKnXnnK war_ar8_re1 ksyncd[9667]: ksyncd_ksync_handle_asyncmsg: *{4,4}
  - Support : 29,265

Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
--ML/DL overall approach

Preprocessing & Parsing: Logs are parsed into separate events

Feature Engineering

--First slice the raw logs into a set of log sequences by using different grouping techniques

- **fixed windows, sliding windows, and session windows**

--Each log sequence, we generate a feature vector (event count vector), which represents the occurrence number of each event.

--All feature vectors together can form a feature matrix, that is, a event count matrix.

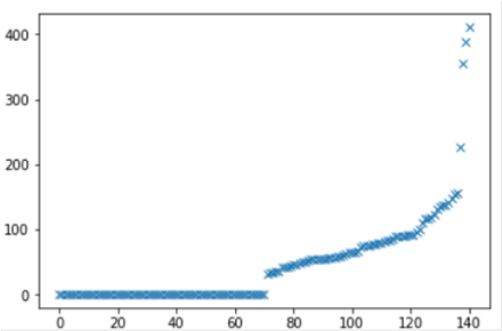
--Each Feature Vector is labeled as normal or not anomaly (if labeling is possible)

ML/DL approaches

the feature matrix can be fed to machine learning models for training, and thus generate a model for anomaly detection.

The constructed model can be used to identify whether or not a new incoming log sequence is an anomaly.

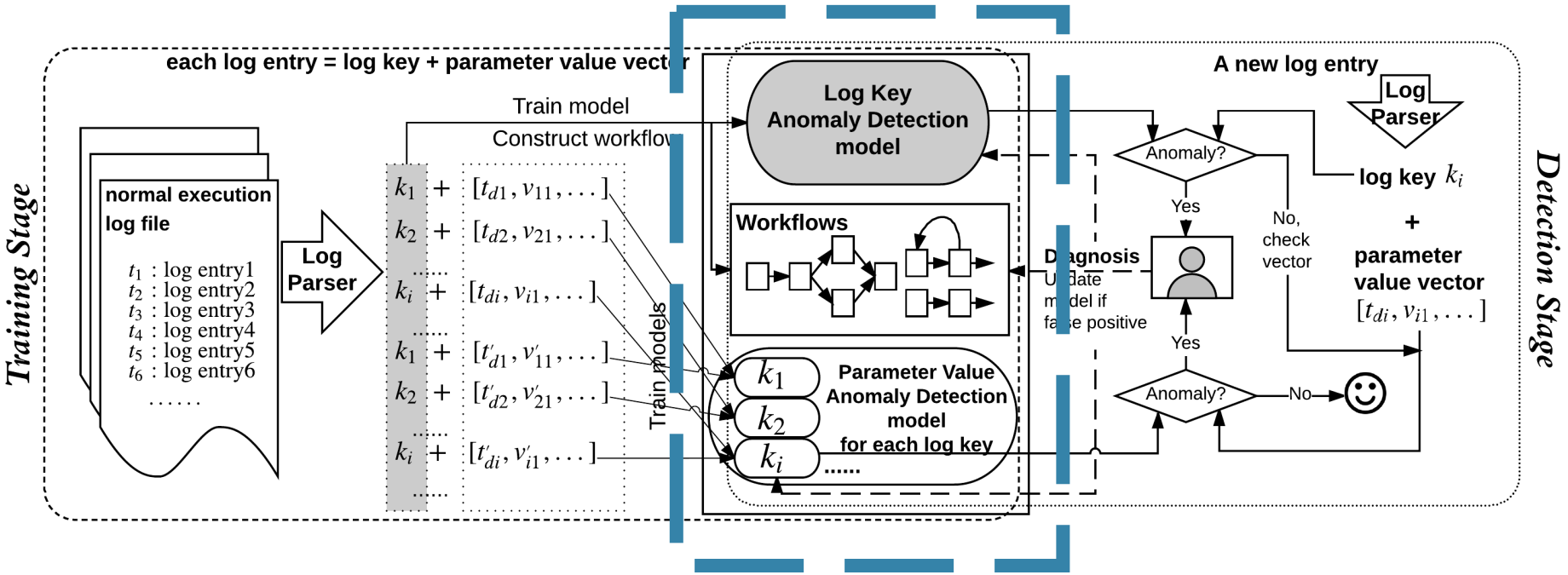
Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
--e.g. of ML/DL approach: PCA for Anomaly detection on logs




```
SCORE : 225.92981563167595
2017-12-31 03:33:08
94
['79b54b1e', '41b2177a', '1e8509e8', 'ec9674ef', 'ce17dc32', '05ede55b', '41b2177a', '1e8509e8', '41b2177a', '283aa
cfc', '1e8509e8', '283aacfc', '9ed475e7', '283aacfc', '423be0f1', 'c7e15a65', '41b2177a', '1e8509e8', '41b2177a', '
1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '41b2177a', '1e8509e8', '1e8509e8', '41b2177a', '1e8509e8', '79b54b1
e', 'ec9674ef', '423be0f1', '9ed475e7', '423be0f1', '9ed475e7', '41b2177a', '662cbd5c', '1e8509e8', '41b2177a', '1e
8509e8', 'da4b2668', 'c8654b95', 'fa08301e', '625ba28a', '41b2177a', '41b2177a', '1e8509e8', '9ed475e7', '1e8509e8
', 'c7e15a65', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '662
cbd5c', '96778e8c', '968823f0', 'fa08301e', '79b54b1e', '625ba28a', '9ed475e7', '41b2177a', '1e8509e8', 'ec9674ef',
'41b2177a', '1e8509e8', '662cbd5c', 'bbbdc961', '79c31df7', '3ed159a1', 'c7e15a65', 'fa08301e', '41b2177a', '625ba2
8a', '1e8509e8', '41b2177a', '1e8509e8', '7aceccd4', '7aceccd4', '7aceccd4', '5b8c37de', 'ae692774', 'e6fec0fc', 'e
c9674ef', '79b54b1e', 'c7e15a65', '07d3040b', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8']
--------------------------------------------------------------------------------------------------------------
SCORE : 410.44004473490475
2017-12-31 03:33:20
190
['41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '283aacfc', '41b2177a', '41b2177a', '9ed475e7', '1e8509e8', '1e850
9e8', '41b2177a', '1e8509e8', 'ce17dc32', '41b2177a', '1e8509e8', '05ede55b', '41b2177a', 'c7e15a65', '1e8509e8', '
41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', 'ec9674ef', '283aacfc', '423be0f1', '0af28b7
3', 'c9d42cf9', '5b00132e', '80c1d237', '79b54b1e', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e
8509e8', 'c7e15a65', '41b2177a', '5b8c37de', '5b8c37de', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8
', '9ed475e7', '0bc8f069', '9ed475e7', '662cbd5c', '5de9179d', '41b2177a', 'ec9674ef', '62171cb6', '1e8509e8', 'da4
b2668', '5250c548', '41b2177a', 'c8654b95', '41b2177a', '1e8509e8', '1e8509e8', 'fa08301e', '625ba28a', '9ed475e7',
'41b2177a', '41b2177a', '1e8509e8', '1e8509e8', '41b2177a', '79b54b1e', '1e8509e8', '662cbd5c', '41b2177a', '1e8509
e8', '96778e8c', '41b2177a', '1e8509e8', '968823f0', 'fa08301e', '625ba28a', '41b2177a', '41b2177a', '1e8509e8', '1
e8509e8', '41b2177a', '0af28b73', '1e8509e8', 'c9d42cf9', '5b00132e', '80c1d237', '41b2177a', '1e8509e8', '41b2177a
', '1e8509e8', '41b2177a', '41b2177a', '1e8509e8', '1e8509e8', '41b2177a', '41b2177a', '1e8509e8', '1e8509e8', '41b
2177a', '41b2177a', '1e8509e8', '1e8509e8', '41b2177a', '1e8509e8', 'c7e15a65', '41b2177a', '1e8509e8', '41b2177a',
'1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', 'ec9674ef', '41b2177a', '1e8509
e8', '41b2177a', '41b2177a', '1e8509e8', '1e8509e8', '41b2177a', '1e8509e8', 'e6fec0fc', '1a49606d', 'cbe63b7d', '7
9b54b1e', '529c6509', '41b2177a', '10ad90ed', '1e8509e8', '41b2177a', 'c3d8940e', 'c3d8940e', '1e8509e8', '5925071c
', '41b2177a', '41b2177a', '41b2177a', '1e8509e8', '1e8509e8', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8
509e8', '9ed475e7', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', '1e8509e8', '41b2177a', 'c7e15a65',
'1e8509e8', '0af28b73', 'c9d42cf9', '5b00132e', '41b2177a', '80c1d237', '1e8509e8', '41b2177a', '1e8509e8', 'ec9674
ef', '1a49606d', 'cbe63b7d', 'efe38d3a', '173063c4', '41b2177a', '17b2aa52', '1e8509e8', '79b54b1e', '5b8c37de', 'f
829a8b2', '41b2177a', '1e8509e8', '662cbd5c', '79c31df7', '3ed159a1', 'fa08301e', '625ba28a']
--------------------------------------------------------------------------------------------------------------
```

Predictive Network Maintenance: *Zoom on Anomaly detection for logs*

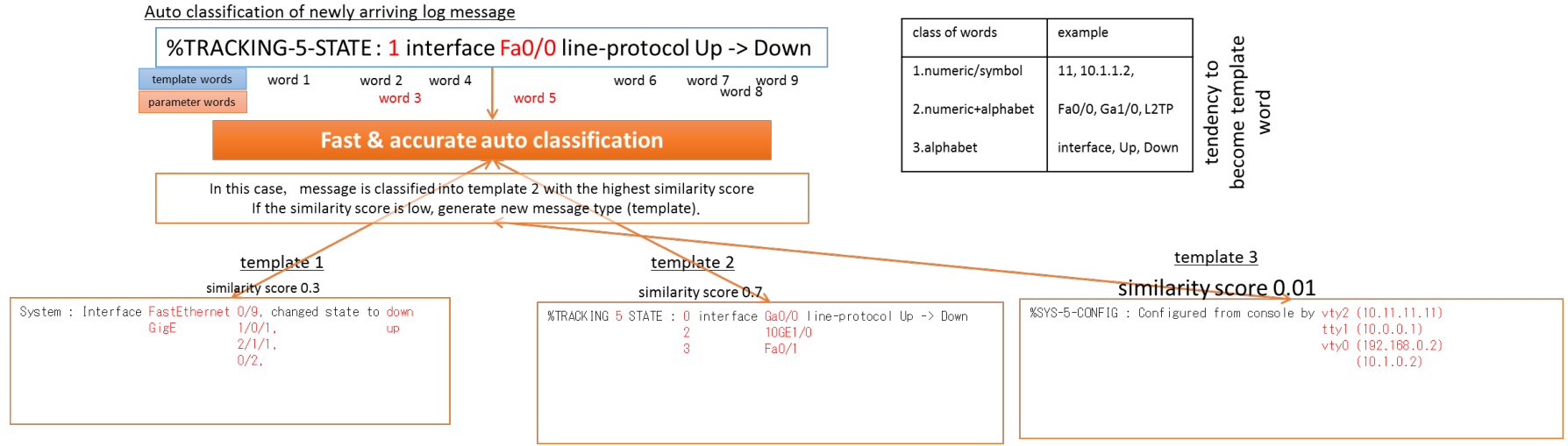
--e.g. of ML/DL approach: Deeplog by M. Du, F. Li, G. Zheng, V. Srikumar,



All ref. https://www.cs.utah.edu/~mind/

Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
-- e.g. of approach : NTF* approach for log mining by NTT

- Automatic classification (template extraction) without previous knowledge about log data from unstructured and complex text log messages
  - Fast processing
    - ⇒ Process data from large scale NW data with realistic time (20,000 messages/sec).
    - Online clustering log messages based on similarity score of each message with template
    - Weighting each word by tendency to become template words or parameter words
  - No dependence on vendors, services, or OSs
    - can run on multivendor NW by applying machine learning technique



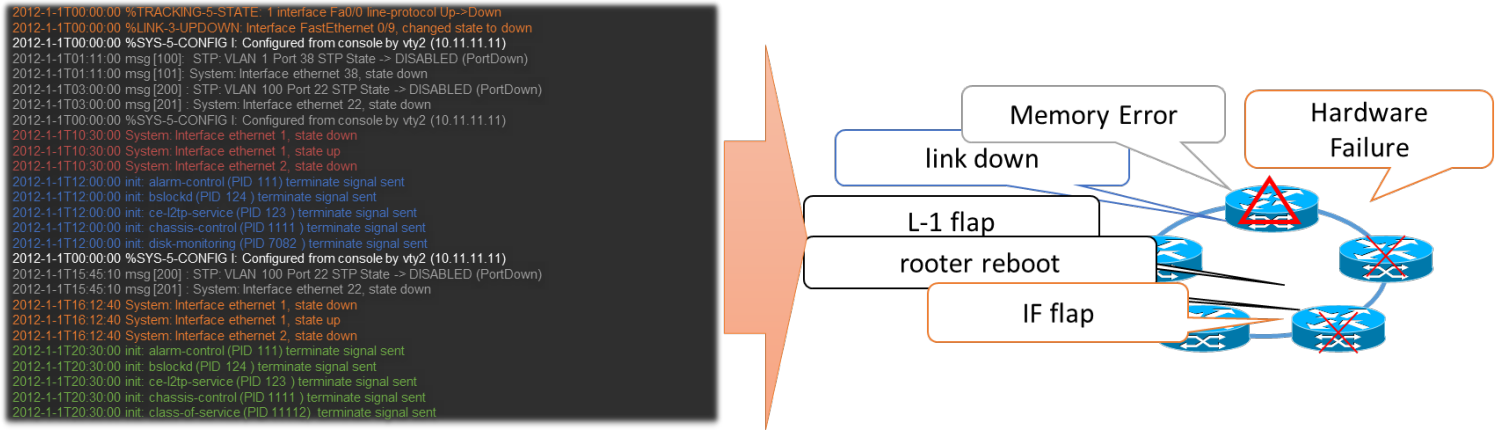
NTF* Non negative Tensor Factorisation

Predictive Network Maintenance: *Zoom on Anomaly detection for logs* -- e.g. of approach : NTF* approach for log mining by NTT

- Extracting *NW event information* from large and diverse NW log data

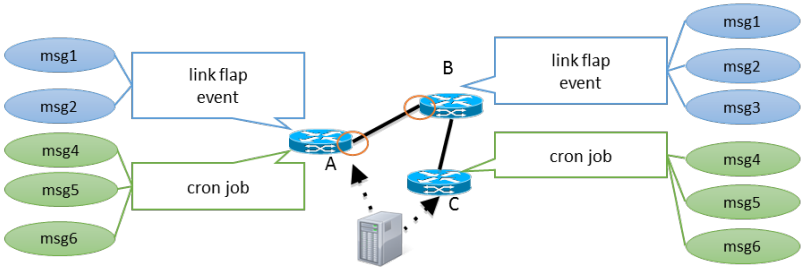
Network events…

- messages associated with the initialization of various process caused by router reboot event
- multiple layer flaps caused by L-1 flap (L-2, OSPF re-convergence, BGP flap, …)
- virtual path dis-connection related to physical machine down



Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
-- e.g. of approach : NTF* approach for log mining by NTT

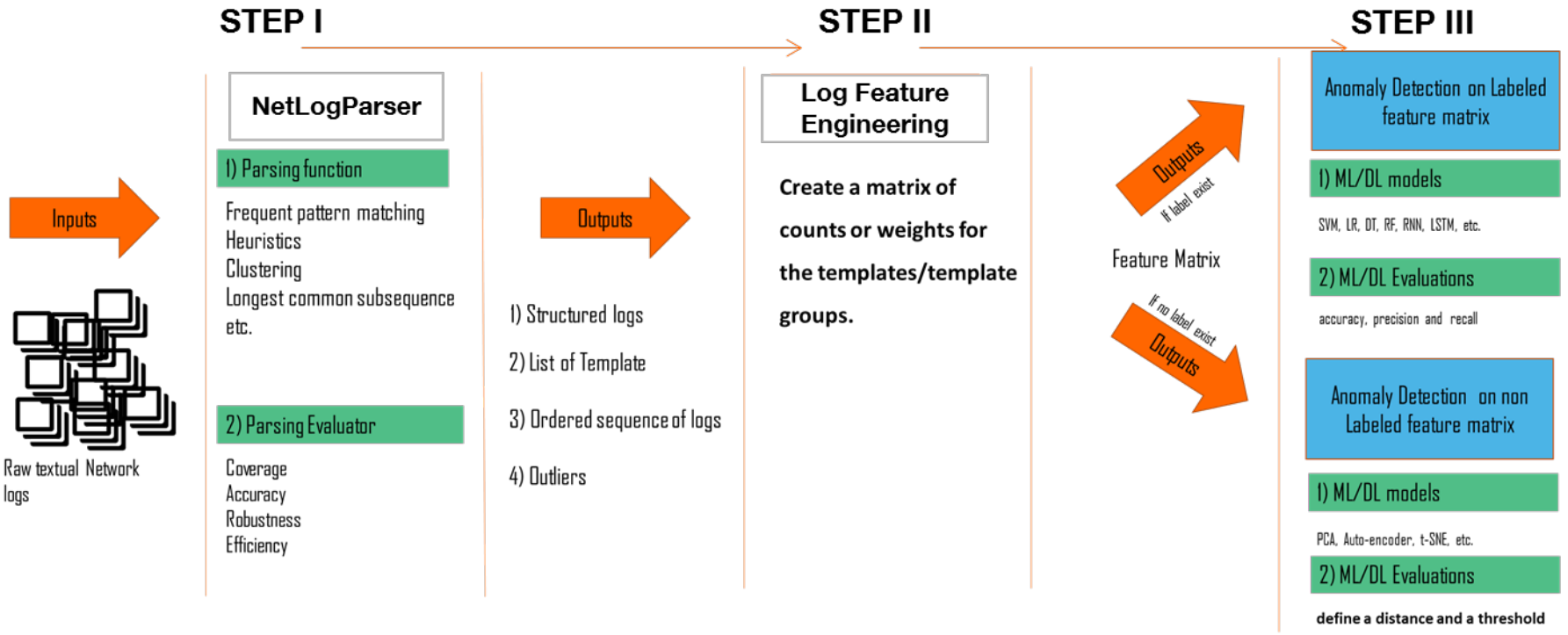
- Representing Log Data as Matrix/Tensor and Factorizing it
- Log data can be considered as a rank-3 tensor
  - types of log messages (log templates), hostname , time
- Observed log data = a ‘superposition’ of NW events



	msg1	msg2	msg3	msg4	msg5	msg6
A	○	○		△	△	△
B	○	○	○			
C				△	△	△

- Extraction of NW events problem ⇒ Tensor Factorization

Predictive Network Maintenance: *Zoom on Anomaly detection for logs*
--Summary of log mining approach based on SOTA analysis



Predictive Network Maintenance: *Zoom on Root Cause Analysis*
--Motivation & high level view

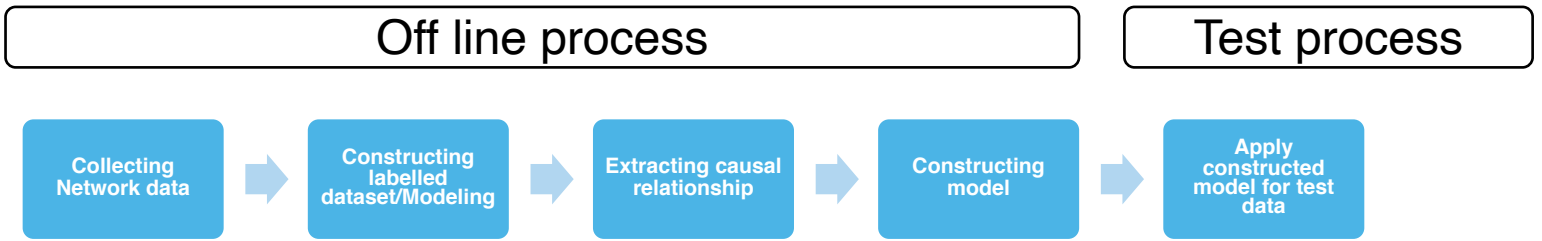
- Motivation: After detection in the network, next step is to identify causes (failed equipment/deterioration factors)
- Task is to extract causal relationship between causes and input data

  knowledge base: using experts knowledge

  Rule base: using IF-THEN rules (Network management Products)

  Model base: using probabilistic model (Bayesian Network)

  ML base: using labeled dataset (Structure learning of Bayesian Network, Classification)
- High level view



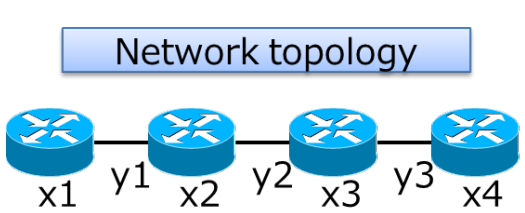
Predictive Network Maintenance: *Zoom on Root Cause Analysis*
--Mathematical formulation

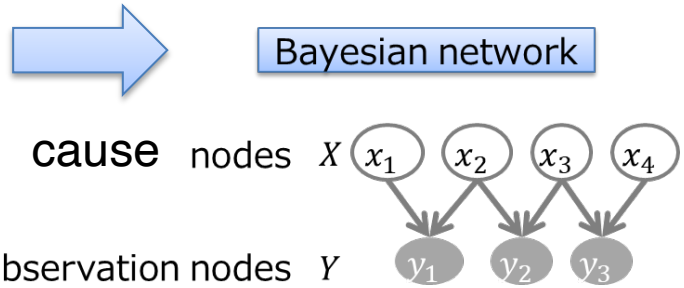
❑ **Problem Formulation: Bayesian network [4]**

- $X = (x_1, x_2, \dots, x_n), x_i \in \{0,1\}$: **cause node (latent node)**
  Denoting cause *i* status
- $Y = (y_1, y_2, \dots, y_m), y_i \in \{0,1\}$: **observation node**
  Denoting observation data *j* status
- $P(X)$ **: representing how often causes occur**
- $P(Y|X)$ **: representing causal relations**

❑ **Estimating cause**

$$\tilde{X} = \underset{X}{\operatorname{argmax}} P(X|Y)$$





[4] S. Kandula, and et.al., "Shrink: A Tool for Failure Diagnosis in IP Network," ACM Sigcom Workshop, 2005

Predictive Network Maintenance: *Zoom on Root Cause Analysis*
--e.g. of approach: machine learning and summarization techniques [5]

- **Motivation:**

  Construct causal model of network events

  → understand the network events and prevent critical events

- **Input data: (time stamp, host type, event type)**

  Host type: VM, Router, Switch

  Event type: Blank, Minor, Major, Critical

- **Predict events in next time window using random forest**

  e.g.: Minor events 55 (column: 55th) generates Critical events 32 (row: 32nd) at 80% in next time window

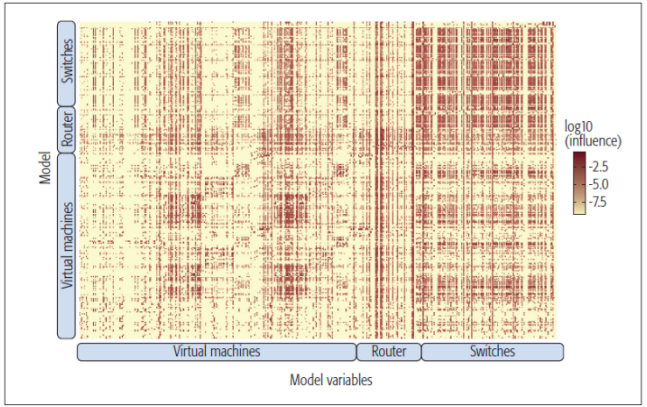


Figure 2. Influence matrix depicted as a heatmap.

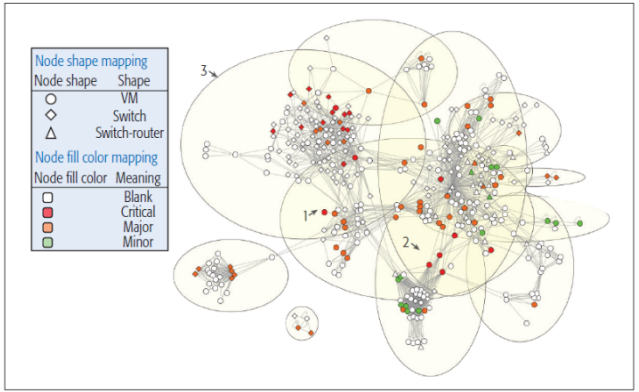


Figure 3. Influence graph of the top 1 percent influences, including communities.

[5] J. M. N. González, et.al.,"Root cause analysis of network failures using machine learning and summarization techniques," IEEE Communication Magazine 2017

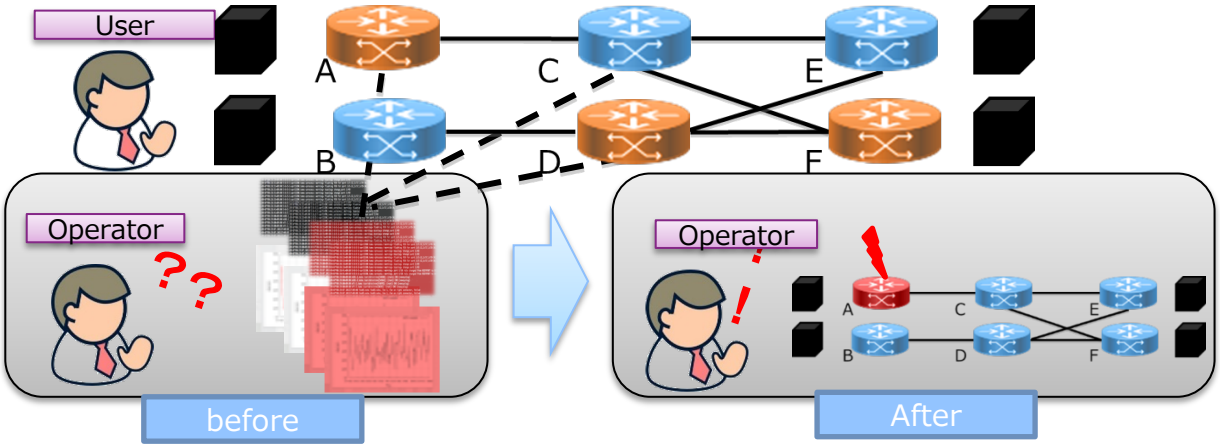
Predictive Network Maintenance: *Zoom on Root Cause Analysis*

--e.g. of approach: NTT approach for root cause analysis

- Root cause analysis for network operators who are troubled with managing operation from massive amount of syslog
- Before: Being hard to Localizing failure points

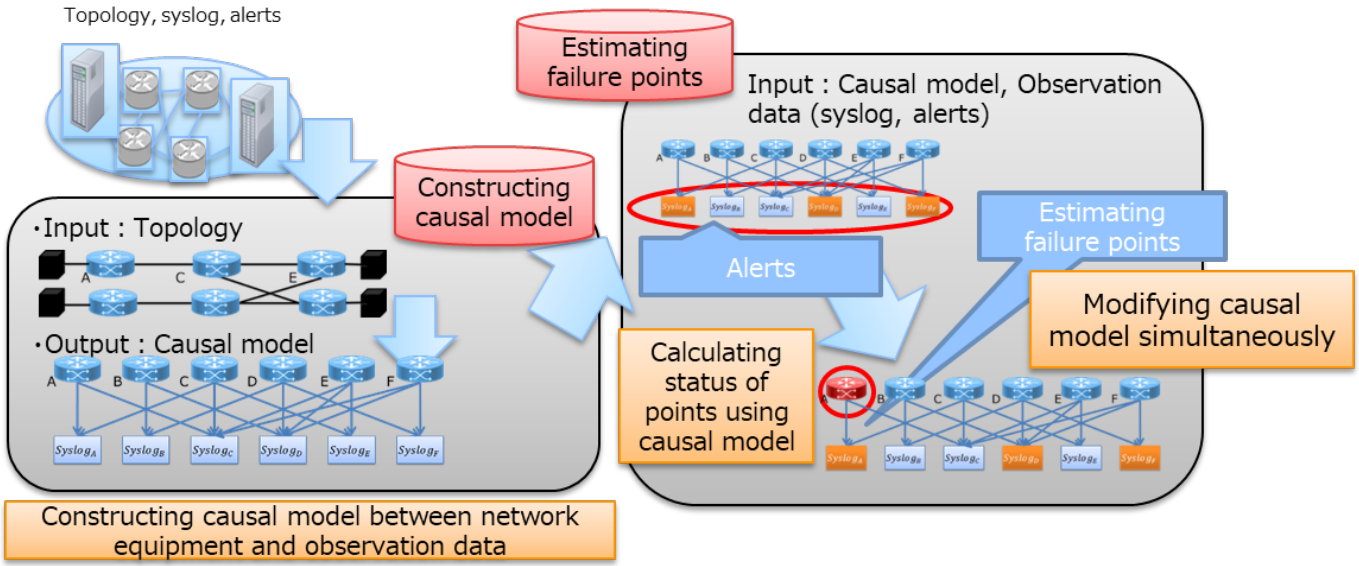
  One of the switch fails generates a massive logs in the network
- After: Making it possible to estimate failure point

  RCA Estimates failure points and show them for operators



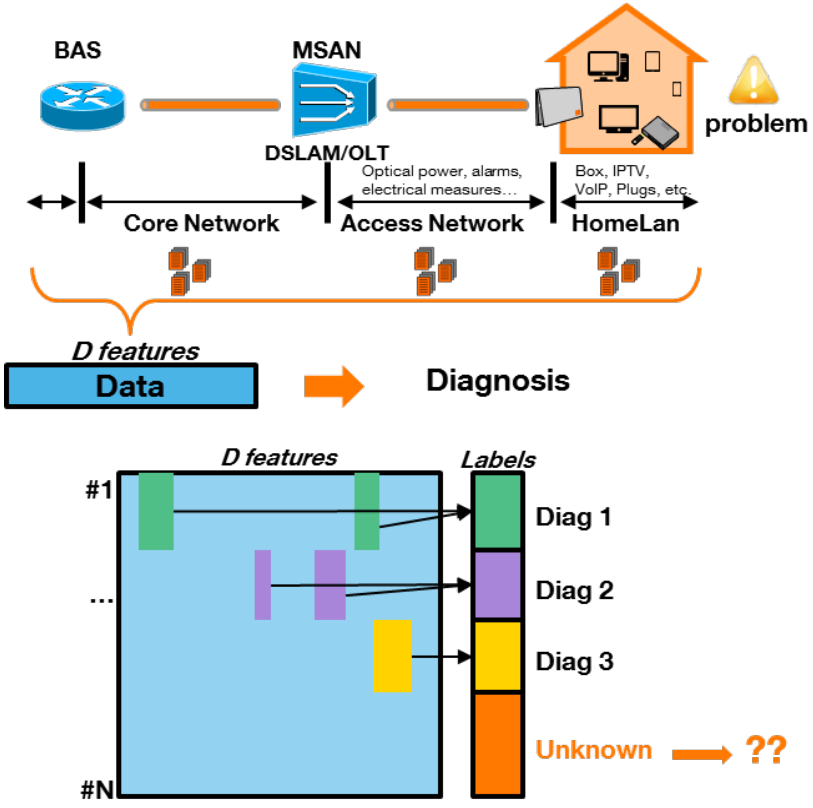
Predictive Network Maintenance: *Zoom on Root Cause Analysis*
--e.g. of approach: NTT approach for root cause analysis [6]

- ❑ **Constructing causal model between network equipment and observation data using topology data**
- ❑ **Estimating failure points from syslog or alerts collected from network**
- ❑ **Modifying causal model simultaneously to adapt unseen failure events**



[6] Yoichi Matsuo, and et.al., "Root-Cause Diagnosis for Rare Failures using Bayesian Network with Dynamic Modification ", IEEE ICC, 2018

Predictive Network Maintenance: *Zoom on Root Cause Analysis*
--e.g. of approach: Orange approach for root cause analysis



Context

- **Each diagnosis has a technical pattern.**
  - Ex 1: low optical power + several ONT alarms.
  - Ex 2: Incompatible firmware version between 2 equipments.

➢ **How can we highlight patterns of new types of failure ?**

Problems

- **A network is sometimes hard to model.**
  - See [1] for a Bayesian Network built for GPON-FTTH.
- **New type of failure may arise regularly.**
  - The solution needs to be flexible.
- **Large feature space (D > thousands).**
- **The number of new failures is unknown (K).**
- **Traditional clustering techniques may lead to irrelevant (trivial) clusters.**

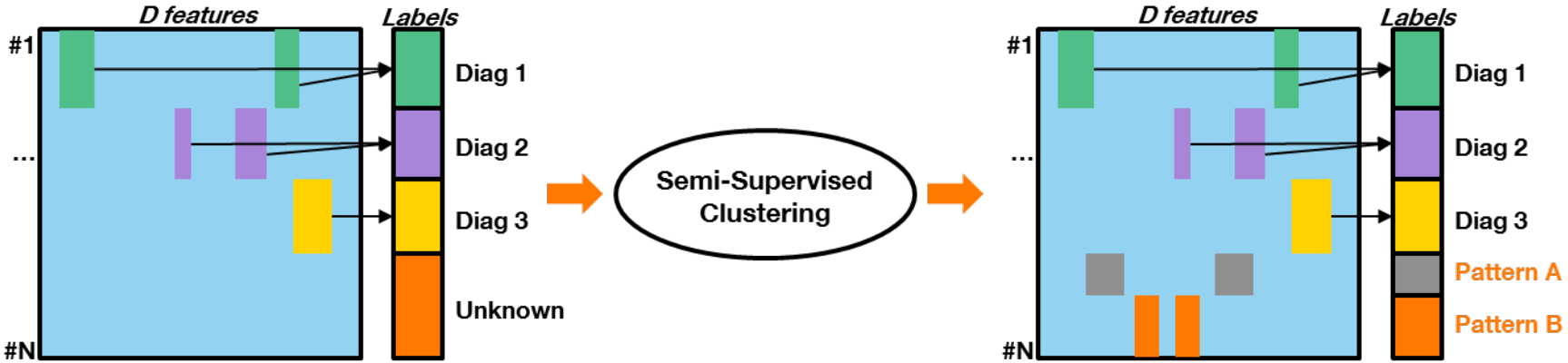
[1]: Tembo S., Vaton S., Gosselin S. Courant JL, Beuvelot M., *Model-based probabilistic reasoning for self-diagnosis of telecommunication networks: application to a GPON-FTTH access network*, JNSM 2017

Authors: Joachim Flocon-Cholet, Amine Echraibi & Stéphane Gosselin

Predictive Network Maintenance: *Zoom on Root Cause Analysis*
--e.g. of approach: Orange approach for root cause analysis

Solution

- **Development of a Bayesian Mixture Model for Semi-Supervised Clustering**
  - ✓ Relevant clusters: make use of some knowledge about the data to guide the clustering process.
  - ✓ Number of clusters (K): infer the right number of clusters from the data thank to the Dirichlet Process.
- **See [2], [3] for details and public implementation.**



[2]: Echraibi A., Flocon-Cholet J., Gosselin S., Vaton S., *Bayesian Mixture Models For Semi-Supervised Clustering*, HAL 2019.
[3]: Echraibi A., Flocon-Cholet J., Gosselin S., Vaton S., *An Infinite Multivariate Categorical Mixture Model for Self-Diagnosis of Telecommunication Networks*, ICIN 2020.

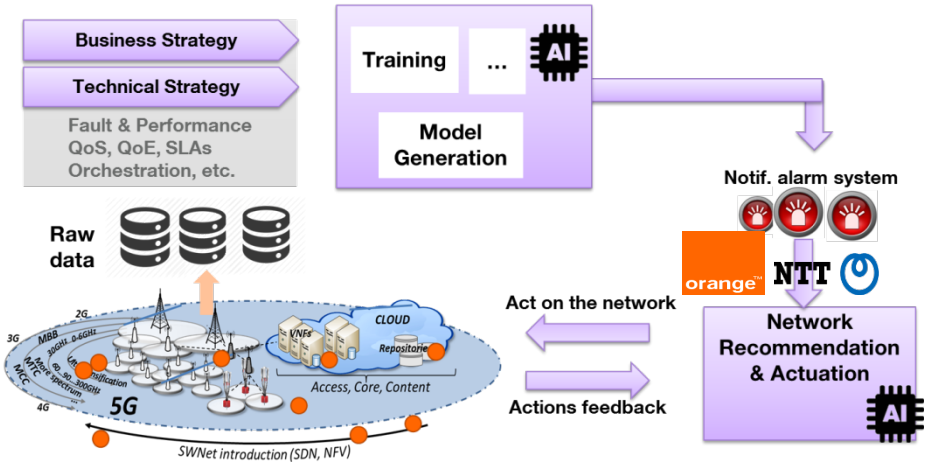
Key messages

Motivation and Scope

For the future of AI model deployment, Orange and NTT jointly evaluate the proof of concept of NW-AI modeling, the applicability of the models, and its distribution.

The scope covers various applications of AI to network management, including log analysis, anomaly detection, root cause analysis in the domains of wireless network, fixed access network, core network, NFV / SDN network.

Orange and NTT joint activities and particular focus on Reinforcement Learning for software networks and beyond 5G.



Acknowledgement

I. Thanks for Stephane Gosselin for leading the NTT & Orange Agreement from Orange side

II. Thanks to my Project team

Aichetou Bouchareb, Moussa Abdi and Alexis Bondu for their involvement on building the Predictive Network Maintenance based on Syslog, Network timeseries, Network Alarms, etc.

I. Thanks for Masakatsu Fujiwara for leading the NTT & Orange Agreement from NTT side

II. Thanks to my Project team

Daisuke Ikegami, Keishiro Watanabe, and Ken Nishimatsu for their involvement on building the Predictive Network Maintenance based on Syslog, Network timeseries, Network Alarms, etc.