O-RAN / ONAP / SDNC

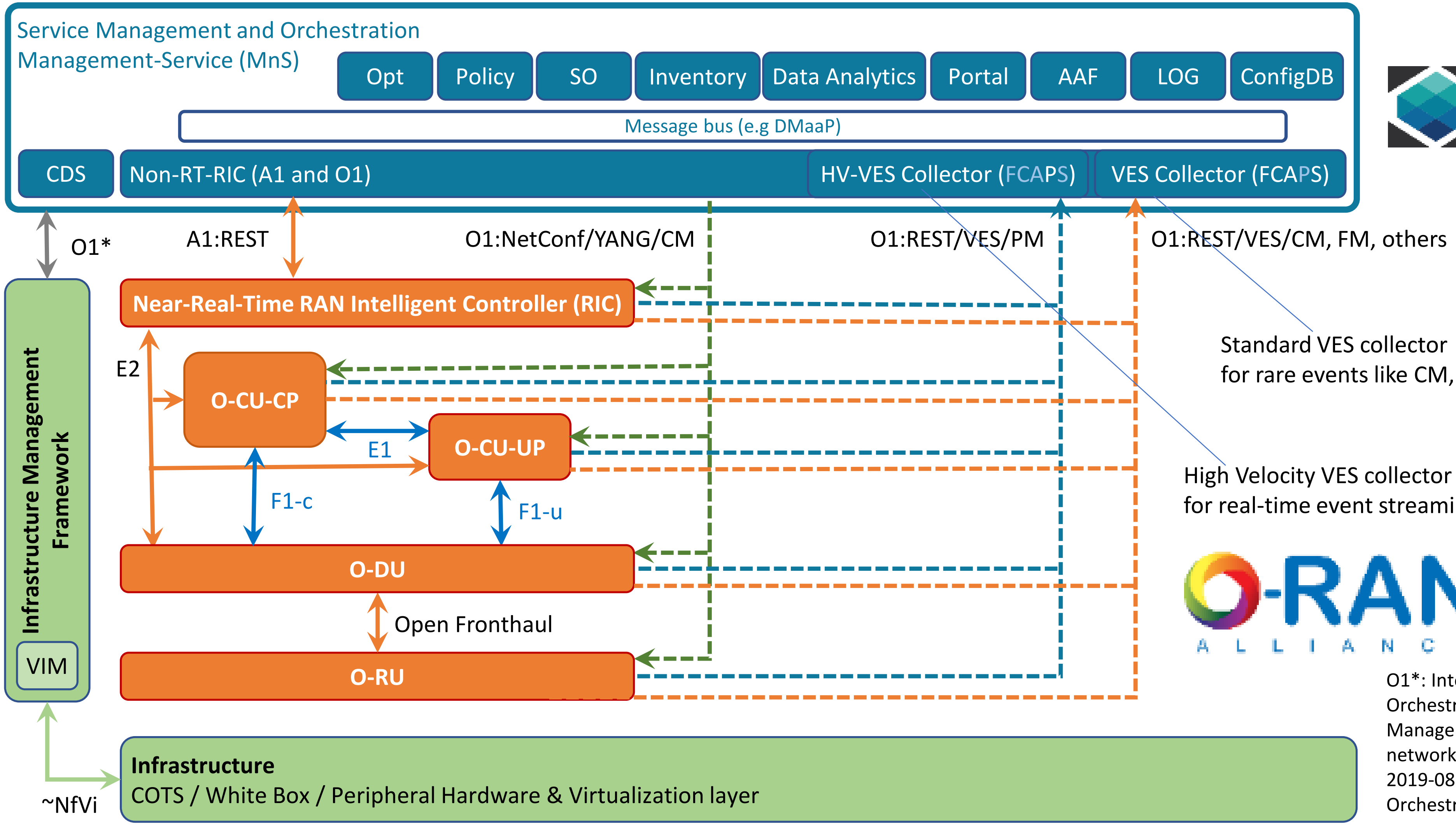
Creating a Data Lake with ONAP

Shabnam Sultana (TU Chemnitz)
Alfons Mittermaier (highstreet technologies)
November 2019

highstreet technologies
Network solutions

O-RAN / ONAP / SDNC

O-RAN Integration into ONAP



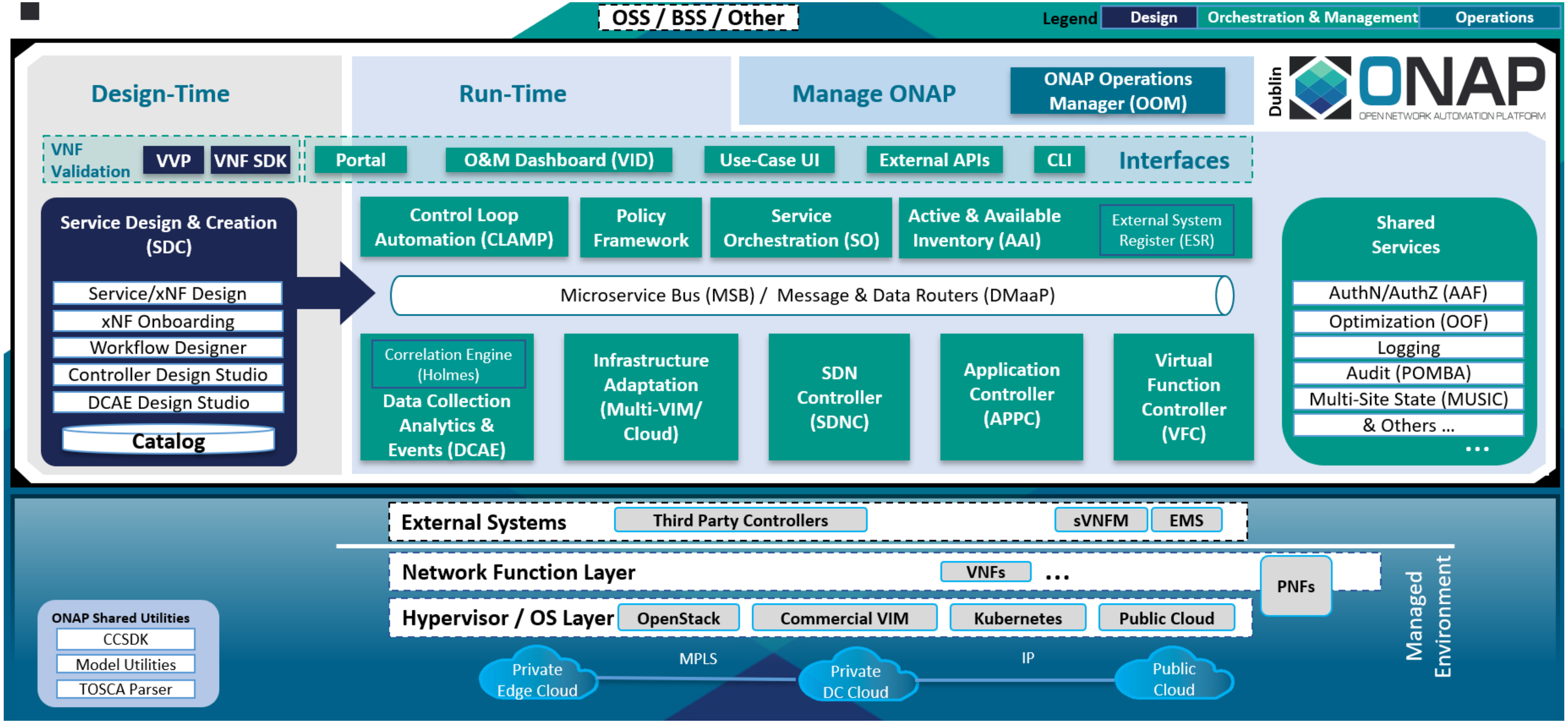
Standard VES collector
for rare events like CM, FM.

High Velocity VES collector (HV-VES)
for real-time event streaming needed for PM.

O1*: Interface between Service Management and Orchestration Framework and Infrastructure Management Framework supporting O-RAN virtual network functions.
2019-08: will be available later in document “O-RAN Orchestration”.

O-RAN / ONAP / SDNC

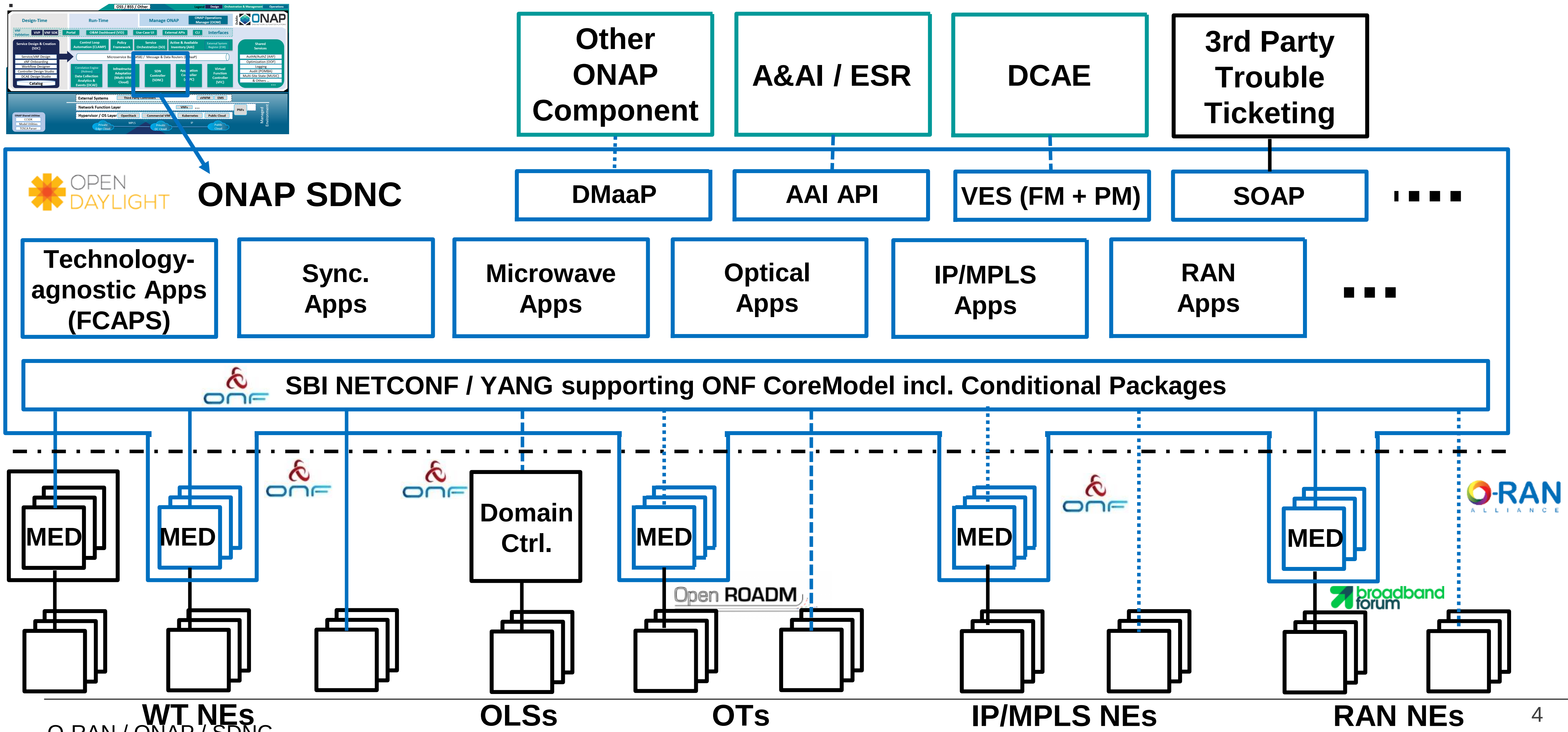
Integration of SDNC within ONAP



O-RAN / ONAP / SDNC

ONAP SDNC as Multi-Technology Domain Controller

highstreet technologies
Network solutions



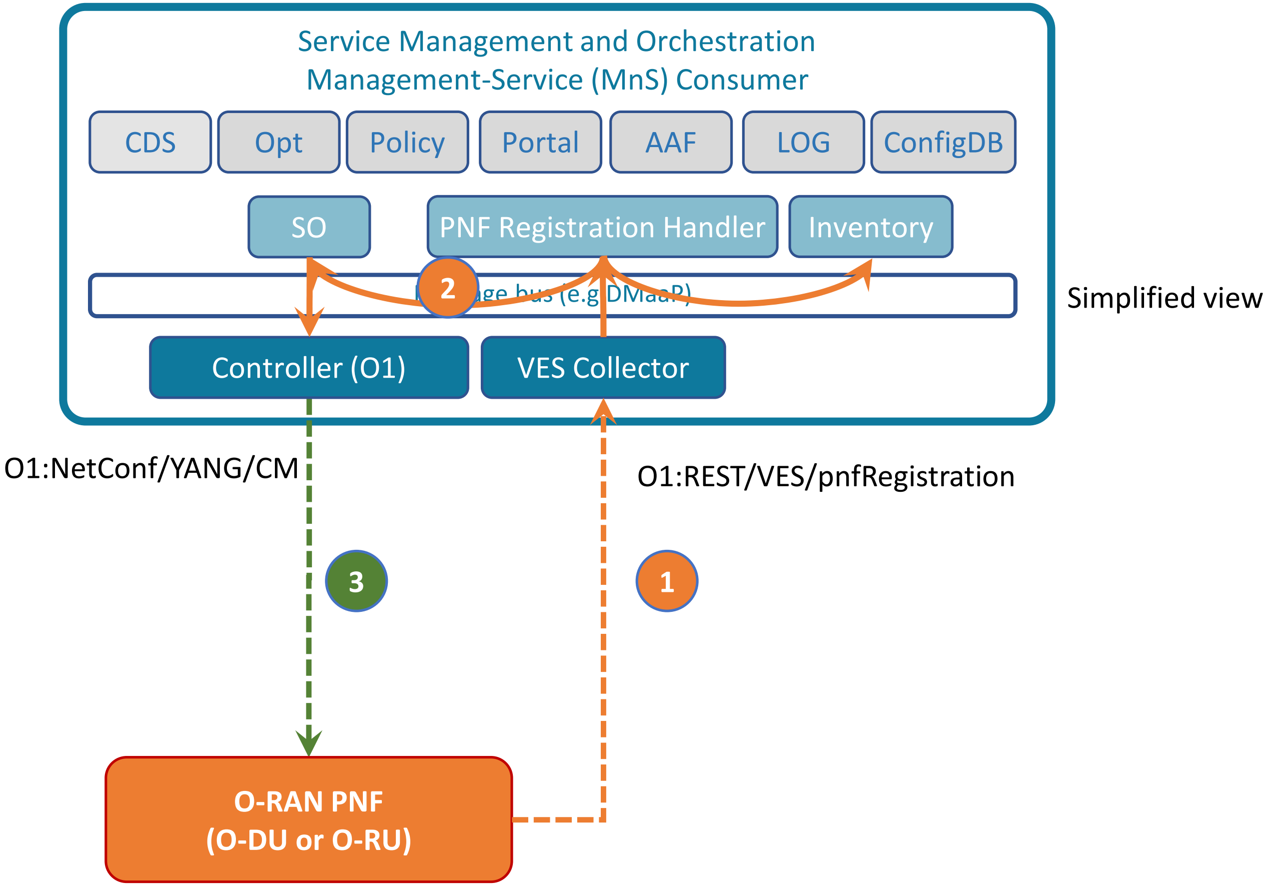
O-RAN / ONAP / SDNC

OAM Use Cases in Dec. 2019

- Physical Network Function (PNF) Plug and Play (PnP)
  (add link to 3GPP and terms in Marge docs)
  https://wiki.onap.org/pages/viewpage.action?pageId=40206485
- Basic configuration (read / write)
- PM Bulk request (add link to 3GPP and terms in Marge docs)
  https://wiki.onap.org/pages/viewpage.action?pageId=40206494
- Basic fault

O-RAN / ONAP / SDNC

Use Case in Dec. 2019: PNF Plug'n'Play Message Flow



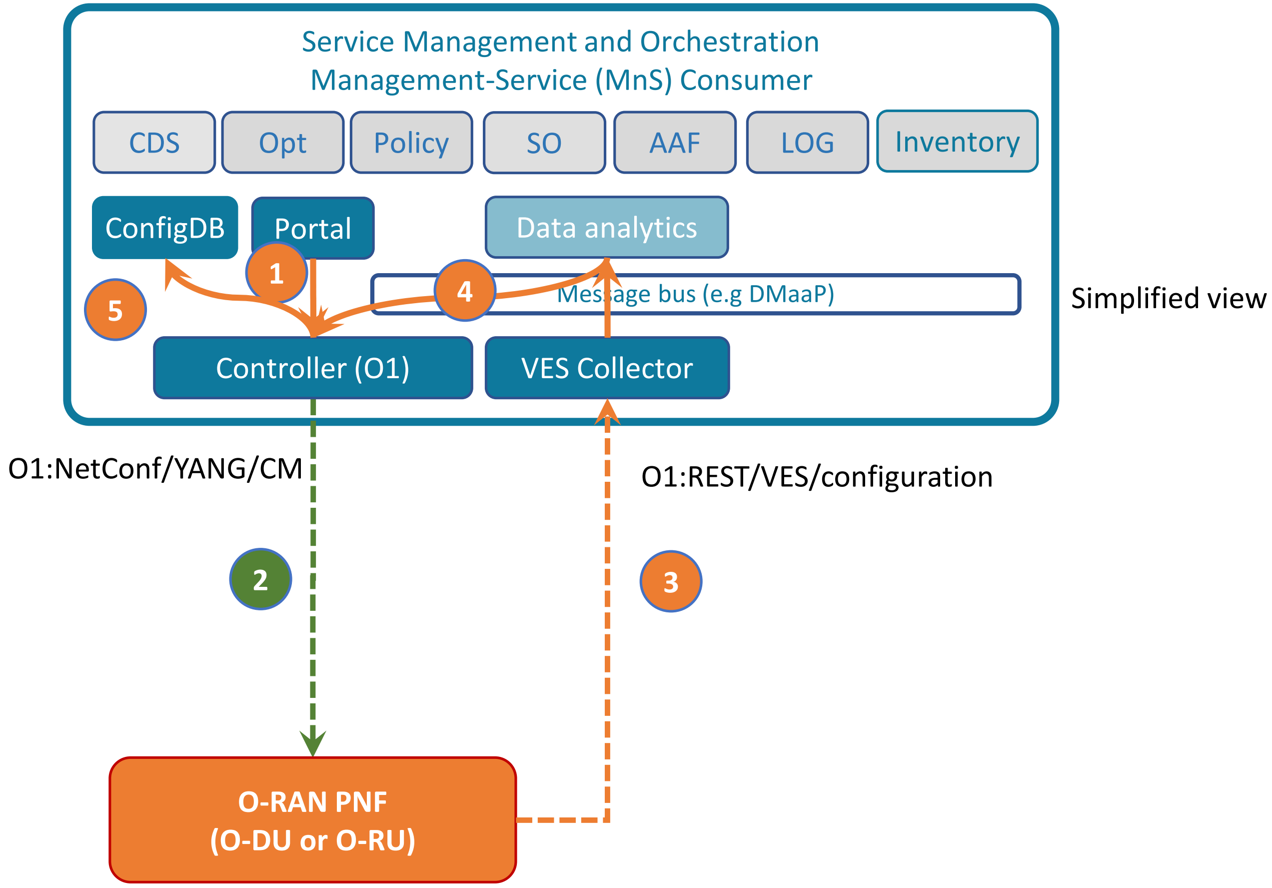
1. O-RAN PNF sends VES pnfRegistration – preferred IPv6/TLS
2. Controller (O1) becomes awareness of the new O-RAN PNF via Message bus
3. Controller (O1) checks NetConf end-point on the O-RAN PNF (hello-message) – preferred: IPv6/TLS

Open topics:

- Dynamic VES subscription mechanism
  - Under discussion by O-RAN and 3GPP
  - Simplification for Demo: pre-configuration of the O-RAN PNF with necessary VES collector information (IP, credentials)

O-RAN / ONAP / SDNC

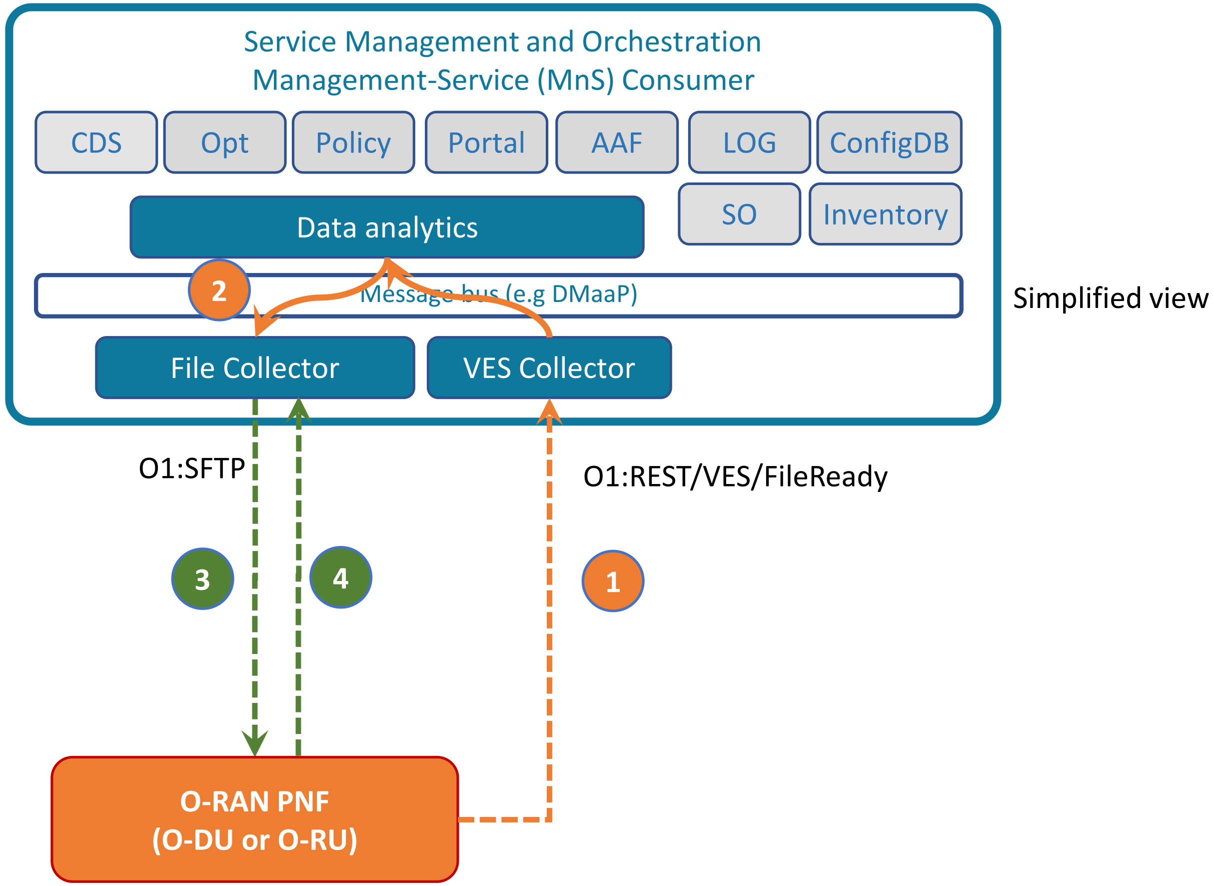
Use Case in Dec. 2019: Basic Config.



1. Operator triggers a modification of configuration data on selected O-RAN PNF
2. Controller (O1) triggers the change via IPv6/TLS(NetConf
3. O-RAN PNF processes the edit-conf and after successful processing a configuration VES message is send.
4. Controller (O1) greps the configuration change from Message Bus (DMaaP)
5. Controller (O1) updates ConfigDB and Portal

O-RAN / ONAP / SDNC

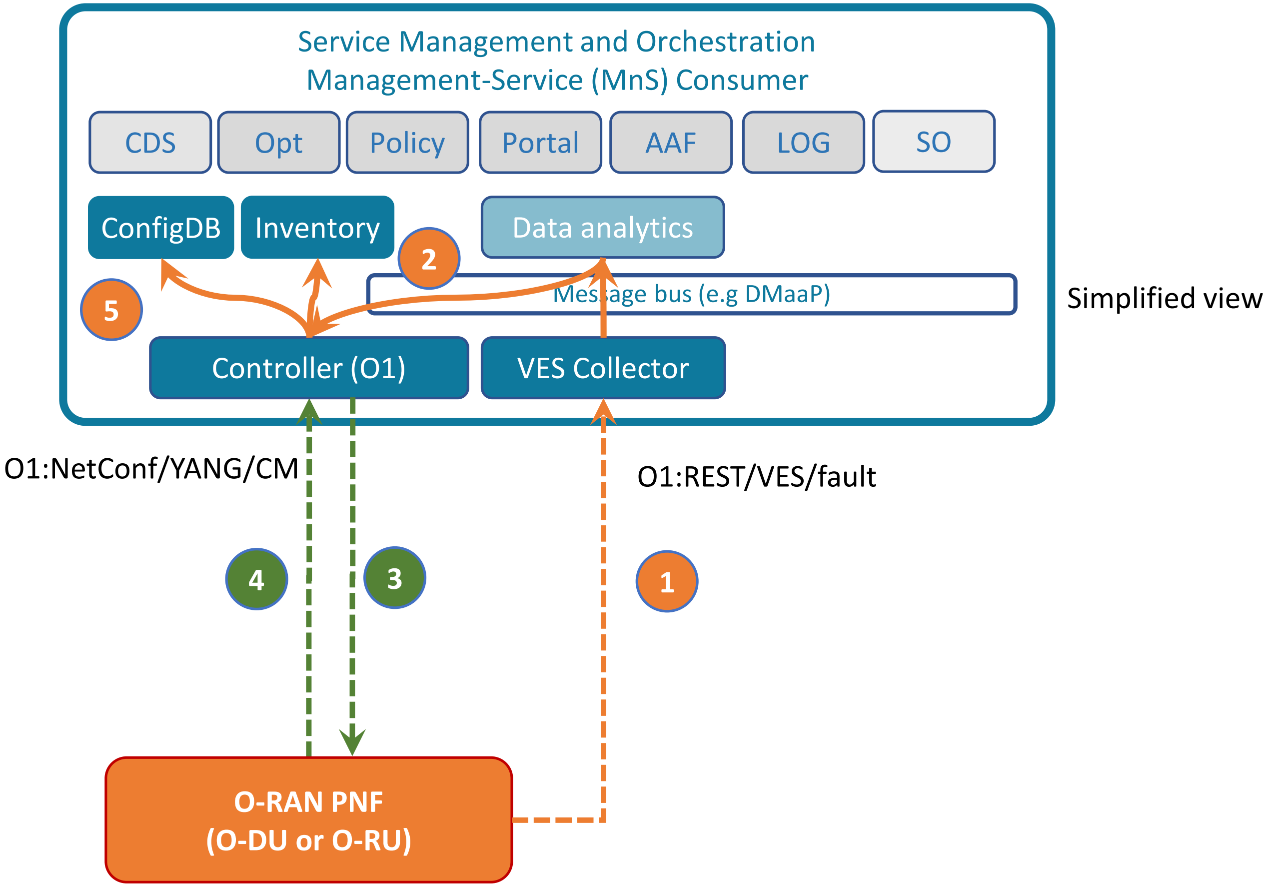
Use Case in Dec. 2019: PM Bulk Request



1. O-RAN PNF sends VES fileRead – preferred IPv6/TLS
2. Data analytics triggers the file transfer.
3. Data analytics requests file transfer – IPv6/TLS/FTPES
4. O-RAN PNF transfers file and Data analytics processes the file; Format is 3GPP XML (TS 32.435) with gzip compression.

O-RAN / ONAP / SDNC

Use Case in Dec. 2019: Basic Fault Message Flow



1. O-RAN PNF sends VES fault – preferred IPv6/TLS
2. Controller (O1) requests configuration data of affected Managed Object Instance.
3. Controller (O1) requests affected configuration preferred: IPv6/TLS
4. Controller (O1) receives configuration data
5. Controller (O1) updates other ONAP components

O-RAN / ONAP / SDNC

Use Case Botnet Detection – Data required from the network

highstreet technologies
Network solutions

Most commonly used features from an IP router

No	Feature	Description
1	SrcIP	Source IP address
2	DstIP	Destination IP address
3	SrcPort	Source Port
4	DstPort	Destination Port
5	AppName	Application Name
6	Protocol	IP protocol
7	Duration	Flow duration
8	TotalSrcBytes	Total source bytes
9	TotalDstBytes	Total destination bytes
10	TotalBytes	Total Bytes
11	TotalSrcPkts	Total source packets
12	TotalDstPkts	Total destination packets
13	TotalPkts	Total packets

Source:http://www.cs.utsa.edu/~shxu/socs/Milcom_2019_Gabe_A_Case_Study_of_Using_Deep_Learning_for_Network_Intrusion_Detection.pdf

O-RAN / ONAP / SDNC

Use Case Botnet Detection – Data required from the network

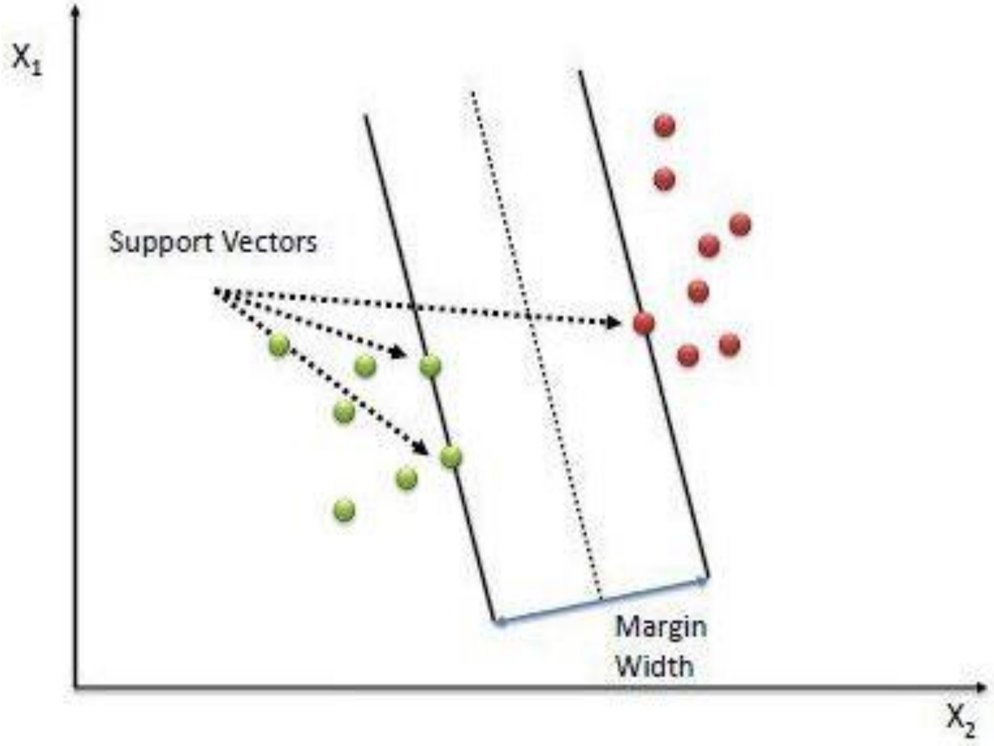
General Features that can be extracted from an OpenFlow switch

No	Feature	Description
1	FlowIN	No. of incoming TCP/UDP/ICMP flows
2	FlowOUT	No. of outgoing TCP/UDP/ICMP flows
3	DistinctSRC	No. of distinct source IP for incoming TCP/UDP/ICMP flows
4	BytesIN	Bytes per incoming TCP/UDP/ICMP flow
5	BytesOUT	Bytes per outgoing TCP/UDP/ICMP flow
6	PacketsIN	No. of packets per incoming TCP/UDP/ICMP flow
7	PacketsOUT	No. of packets per incoming TCP/UDP/ICMP flow
8	SrcPORT	No. of distinct source ports for incoming TCP/UDP flows
9	DstPORT	No. of distinct destination ports for incoming TCP/UDP flows
10	DstPSmallerthan1024	Ratio of destination port ≤ 1024 for incoming TCP/UDP flows
11	DstPGreaterthan1024	Ratio of destination port > 1024 for incoming TCP/UDP flows
12	SymmetricIN	Ratio of symmetric incoming TCP/UDP/ICMP flows
13	SymmetricOUT	Ratio of symmetric outgoing TCP/UDP/ICMP flows

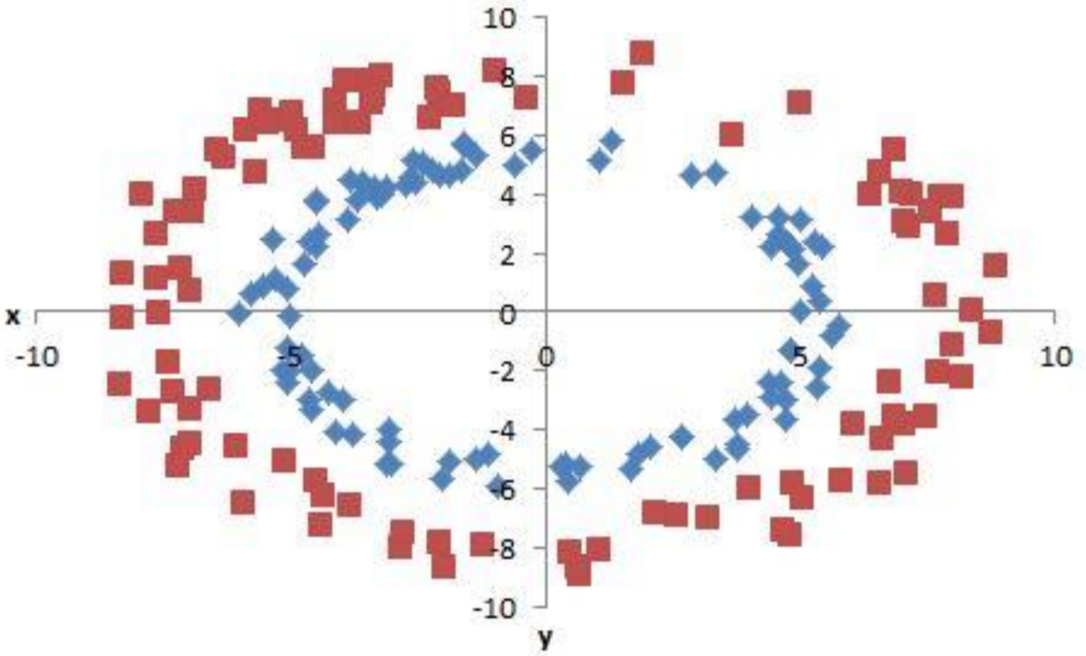
Source: https://arxiv.org/pdf/1611.07400.pdf

Use Case Botnet Detection – Supervised Learning: Classification

Support Vector Machine



Linear SVM



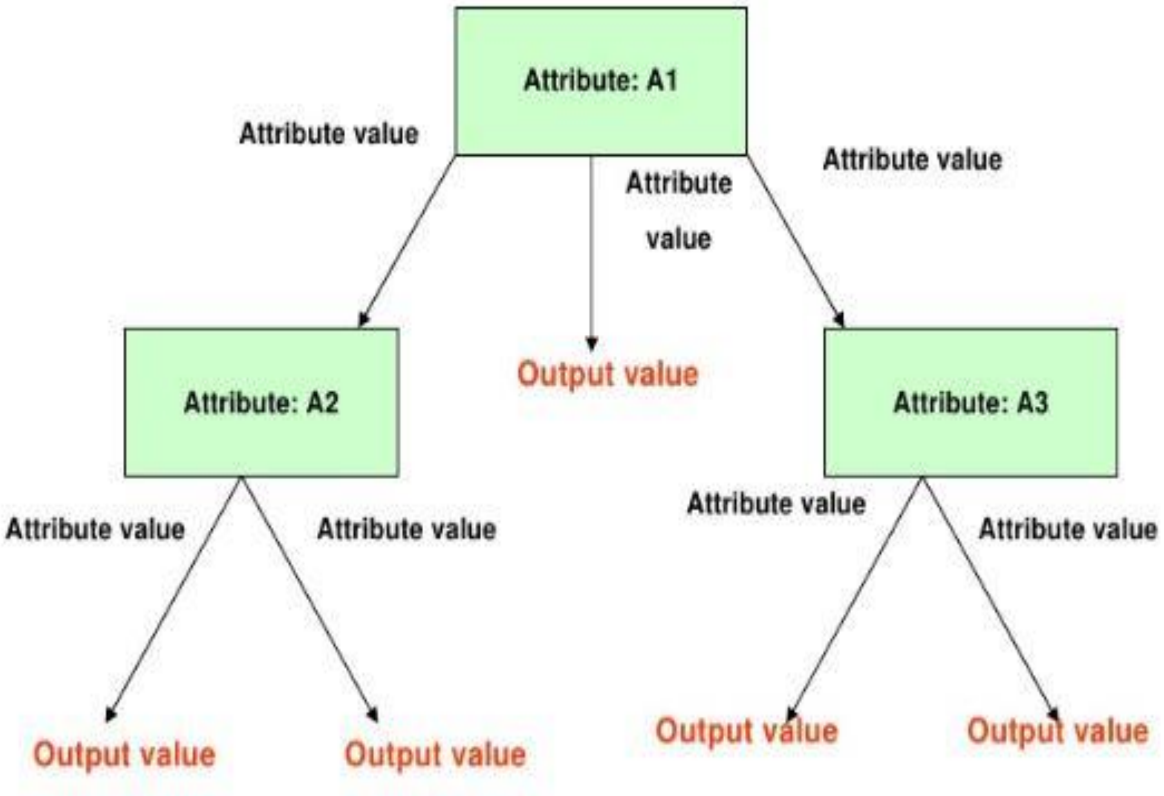
Dual Form SVM

Source:https://towardsdatascience.com/support-vector-machines-svm-c9ef22815589

Use Case Botnet Detection – Supervised Learning: Classification (cont.)

highstreet technologies
Network solutions

Decision Tree



Random Forest Classifiers

1. Creates decision tress from a set of randomly selected subset of training set
2. Aggregate the votes from different decision trees to decide the final class of the test object

Source: https://www.slideshare.net/cnu/machine-learning-lecture-3

Use Case Botnet Detection – Unsupervised Learning: Clustering

highstreet technologies
Network solutions

K Means Clustering

1. Selects random centroids as beginning points of the clusters
2. Each data point is assigned to the nearest centroid based on the Euclidian distance
3. The centroids are recomputed by taking the mean of all the data points assigned to that cluster.
4. Iterate the algorithm between steps 2 and 3 until the centroids are stabilized.

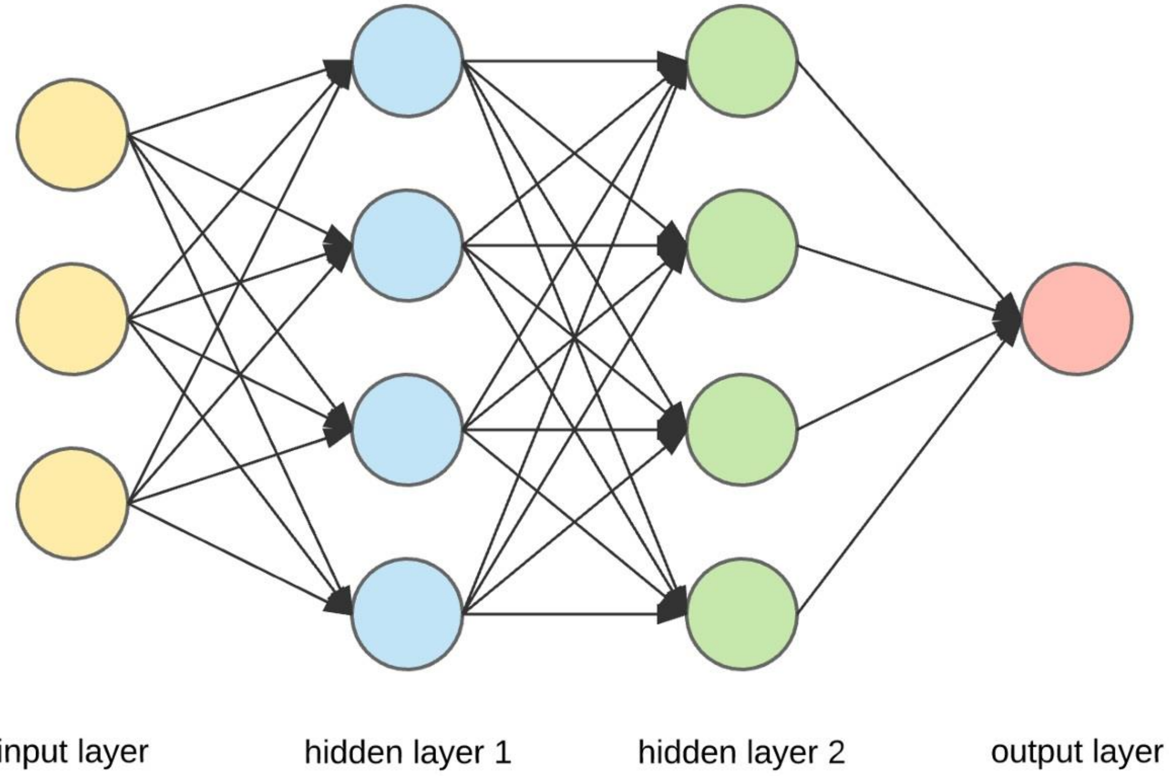
Quarter Sphere Support Vector Machine

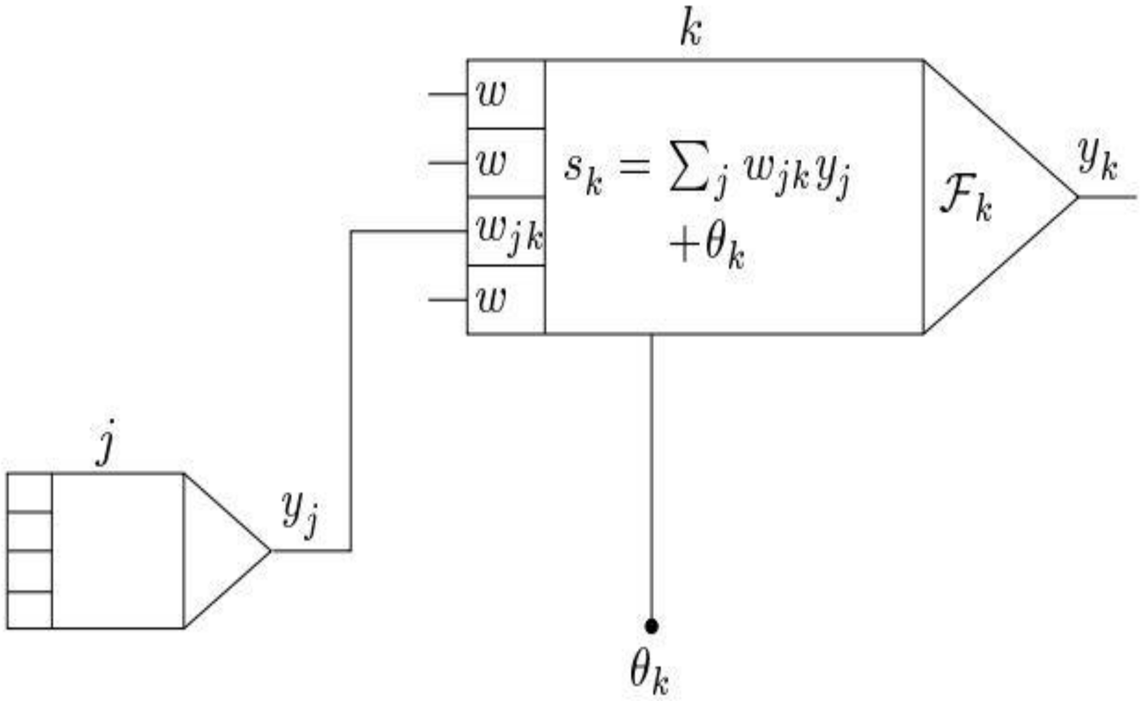
1. Based on the idea of fitting a sphere onto the center of mass of data
2. A threshold determines the radius of the sphere enclosing normal data points
3. A anomaly score is defined by the distance of a data point from the center of the sphere.

Source : https://link.springer.com/content/pdf/10.1007%2F11553595_6.pdf

O-RAN / ONAP / SDNC

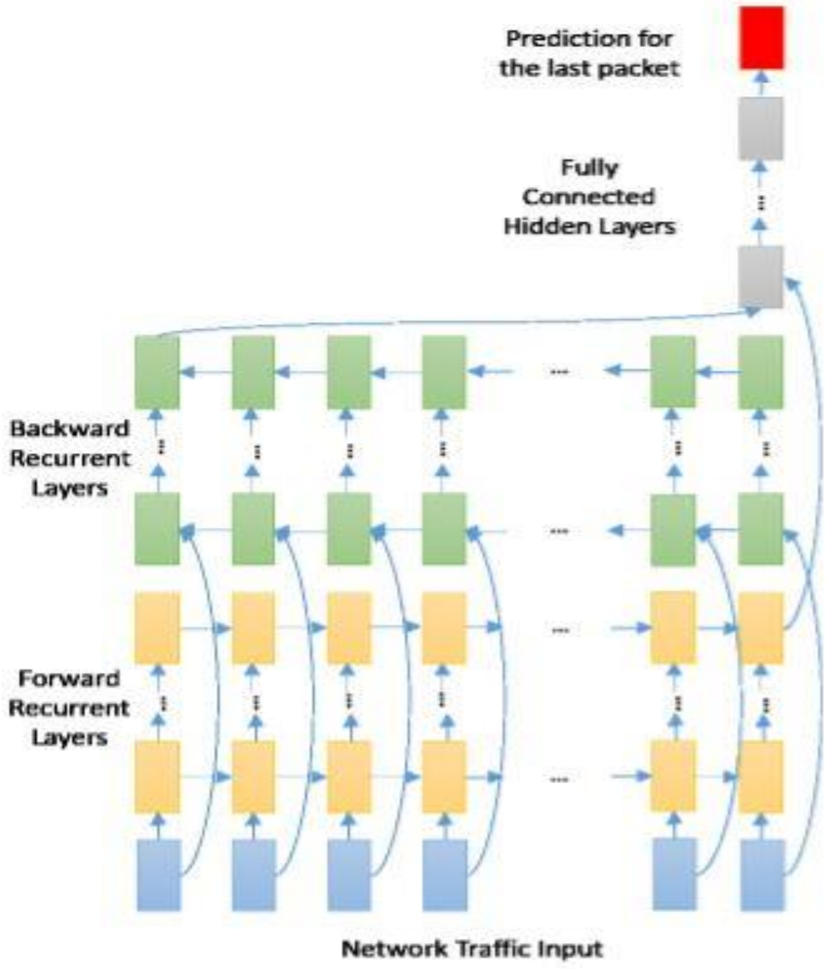
Use Case Botnet Detection – Neural Networks





Source: An introduction to Neural Networks
https://towardsdatascience.com/applied-deep-learning-part-1-artificial-neural-networks-d7834f67a4f6

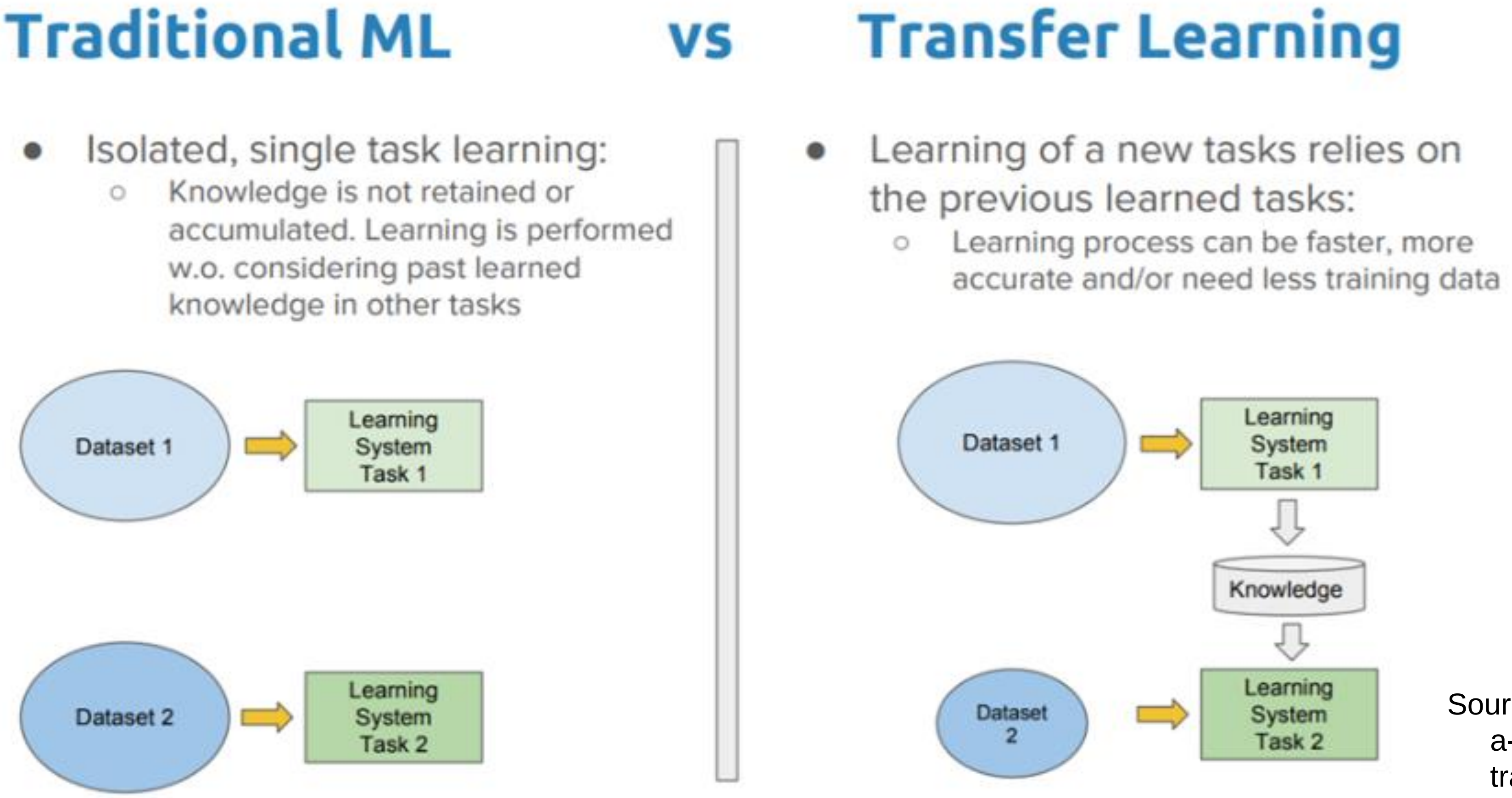
DeepDefense: Identifying DDoS Attack via Deep Learning - X. Yuan, C. Li, X. Li



1. DeepDefense approach to identify DDoS attack based on Recurrent Neural Network (RNN), thus considering historical information
2. DeepDefense reduce the error rate from 7.517% to 2.103% compared with conventional machine learning method in the larger data set.
3. The dataset used is ISCX2012 is provided by UNB in 2012.

O-RAN / ONAP / SDNC

Use Case Botnet Detection – Transfer Learning

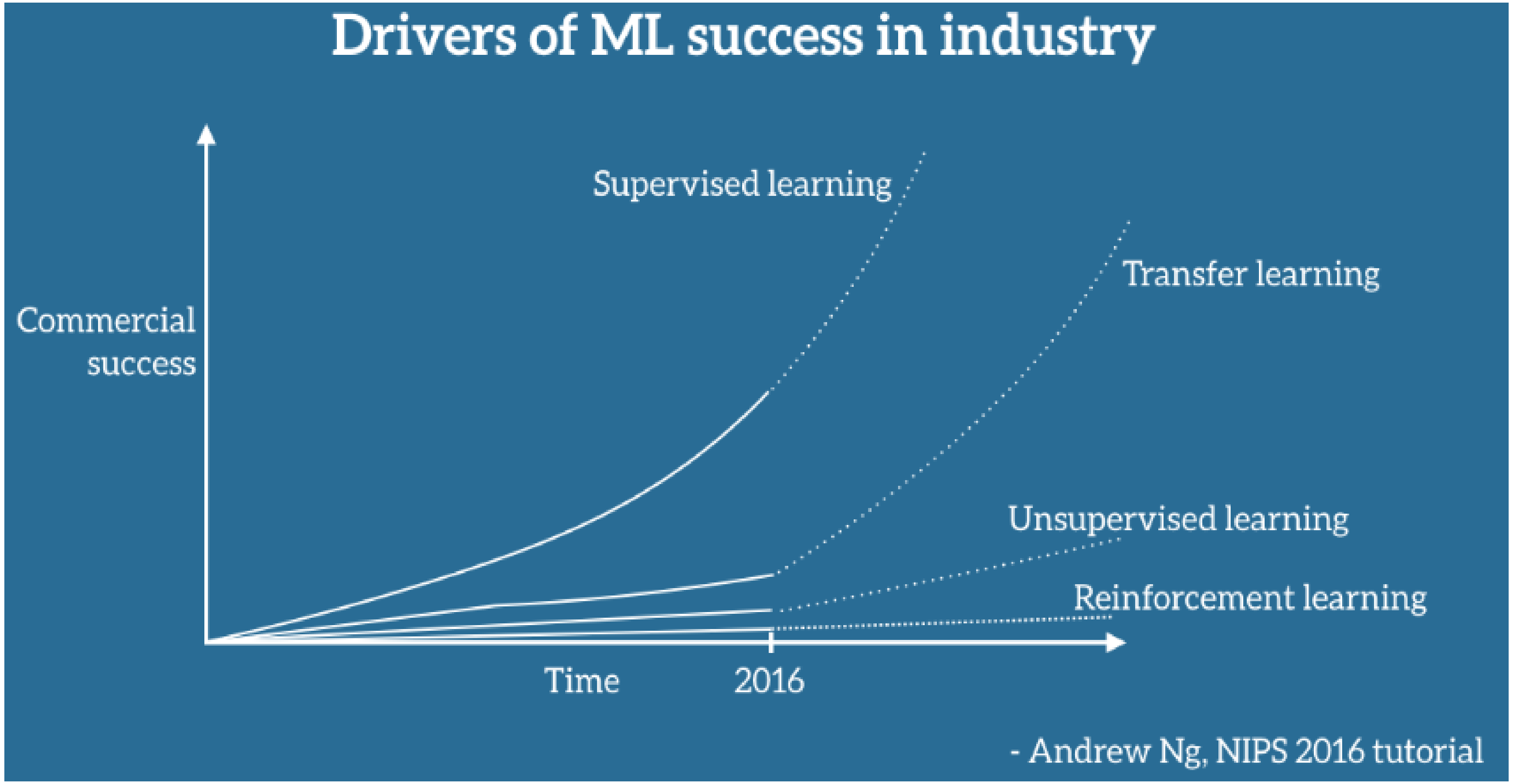


Traditional Learning vs Transfer Learning

Source:https://towardsdatascience.com/a-comprehensive-hands-on-guide-to-transfer-learning-with-real-world-applications-in-deep-learning-212bf3b2f27a

O-RAN / ONAP / SDNC

Use Case Botnet Detection – Future Evolution of Transfer Learning



Andrew Ng 2016 NIPS

O-RAN / ONAP / SDNC

Use Case Wireless Transport – Heavy Rain Prediction

highstreet technologies
Network solutions

- WT links are designed for peak traffic hours and therefore underutilized most of the time.
- One of the typically two polarization planes could be switched off during times of low traffic, thus significantly reducing power consumption.
- However, heavy rainfall increases link attenuation compensated by dynamic reduction of modulation degree and thus bandwidth per link.
- Turning on now needed second polarization plane takes minutes.
- Heavy rain forecast by assessing basic transmission parameters like link attenuation within a geographic area could be used as an indicator for turning on second polarization plane before heavy rain actually arrives.
- Could be combined with rain radar data.
- Currently used 15 minutes performance records probably too infrequent.
- ➢ Performance data streaming via VES messages required.

O-RAN / ONAP / SDNC

Use Case Wireless Transport – Link Deterioration Analysis

highstreet technologies
Network solutions

- WT links may deteriorate for a series of reasons:
  - Clutter: Trees may grow into Fresnel zone.
  - Clutter: Trees may bend into Fresnel zone during strong wind.
  - Other temporary obstructions: Building cranes may move into Fresnel zone.
  - Other temporary obstructions: People or vehicles may move into Fresnel zone every now and then.
  - Other obstructions: Dust on antennas may gradually increase attenuation.
  - Other reasons for degradation: Misalignment of antennas because of inaccurate installation, deformation while and / or after heavy storms, heating of radios due to sun exposure ...
- Currently used 15 minutes performance records probably to coarse-grained.

➢ Streaming of fine-grained performance data via VES messages required.

O-RAN / ONAP / SDNC

Key Takeaways

- AI is being developed all around the world, though often based on historical data.
- Standardization of management interfaces should cover both, RAN and transport.
- AI Framework Architectures (ITU FG ML5G) should go hand-in-hand with open source software projects like ONAP / O-RAN-SC.

- **Let’s connect AI people to our networks!**

Thank you!