SDN as enabler for proactive network operation based on "network science"

SDN-WG meeting, IRTF/IETF 94 (Yokohama)

November 2, 2015

Kohei Shiomoto (NTT)

SDN

Software-Defined Networking (SDN) allows carriers to implement their own managemen t policy by separating the control-plane from the network elements.

- Re-routing on failure and congestion, route opti mization, etc.

SDN-controlled network

Innovative R&D by NTT

Functional requirements

- Traffic Measurement
- Flow classification
- Path computation
- Route enforcement
- QoE management
- Network status update

Performance requirements

- Efficiency, Scalability, Stability, Predictability

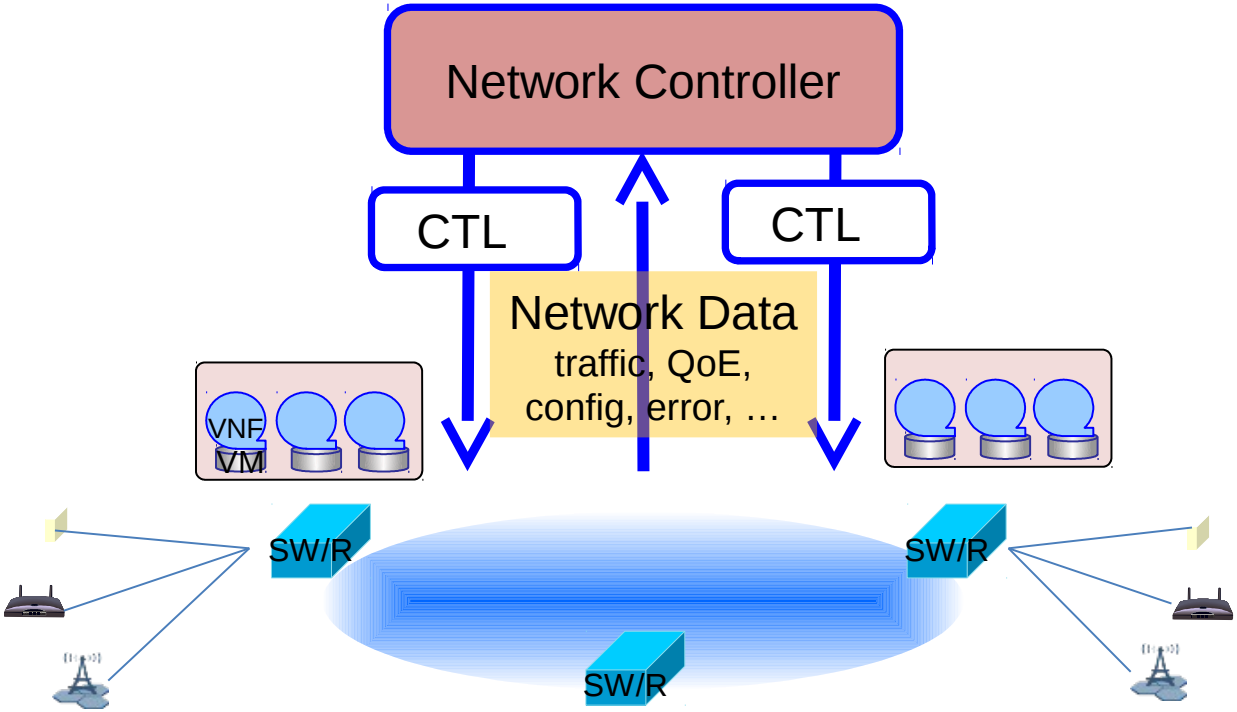
NTT

Macroflow

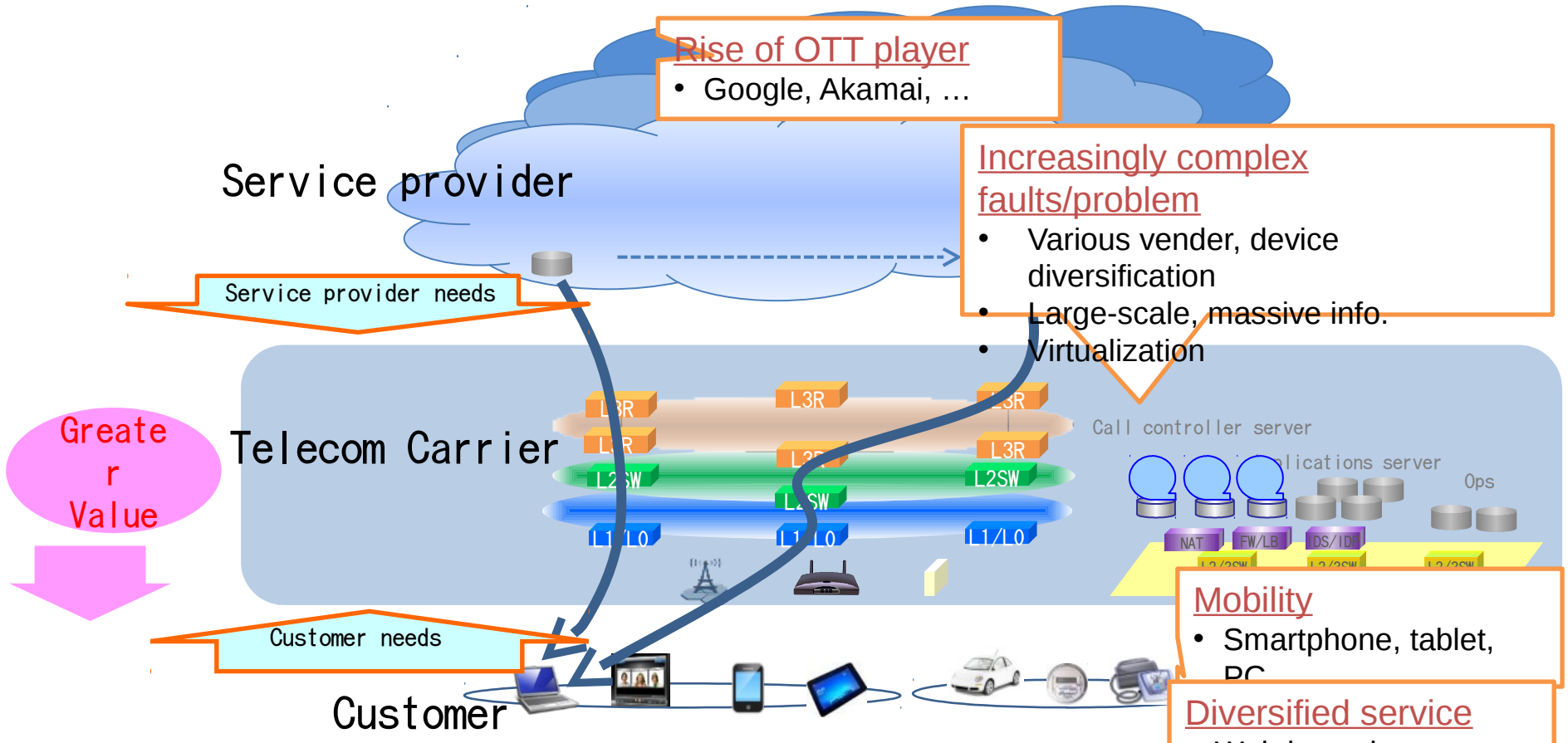
- OD-flow
  - Too coarse for TE
- Microflow
  - Too many for TE
- Macroflow
  - In between OD-flow and Microflow
  - Scalability, Stability, Predictability

Network controller is “Brain”

- Collect data (traffic, QoE, config, error, …)
- Decide actions based on data & policy
- Actuate the network based on the decision

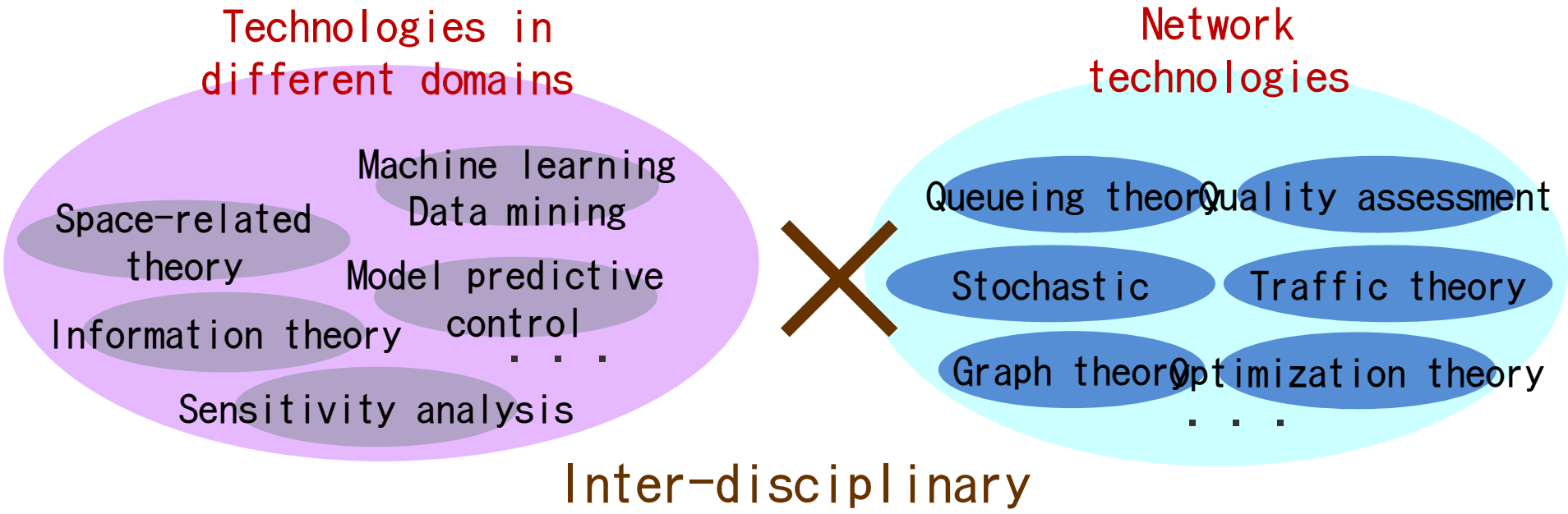


Circumstance surrounding telecom carrier



Network Science

Inter-disciplinary approach by combining various research fields for innovation.



Research topics
Applications of network science

(1) Network analytics

(2) Robust traffic engineering

(3) QoE-centric operation

(4) Disaster-free networks

…

For more detail, see [1].

[1] K. Shiomoto, “Approach to Network Science—Solving Complex Network Problems thr ough an Interdisciplinary Approach,” NTT Technical Review, Vol. 13 No. 9 Sept. 2015
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201509fa1.html

(1) Network analytics

Network analytics

Innovative R&D by NTT

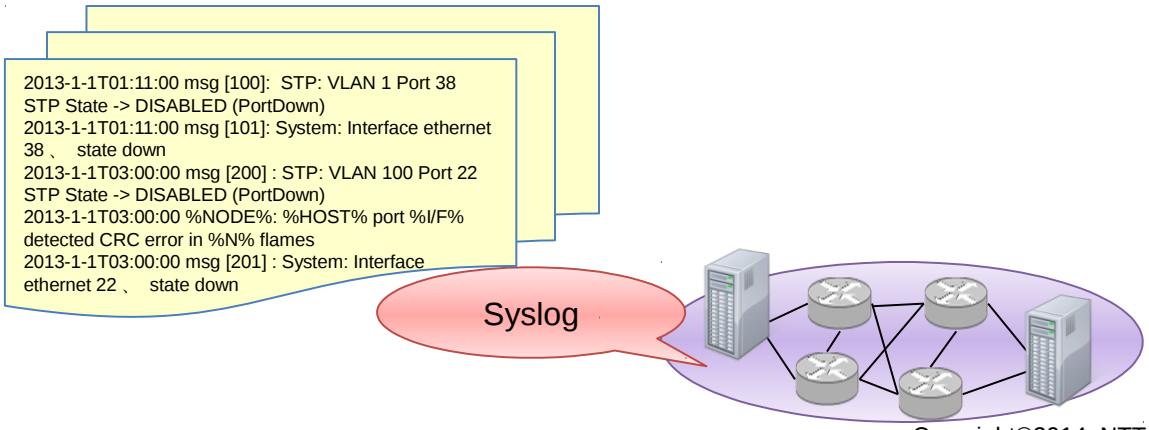
Understand “network behavior” by analyzing d ata to decide actions

- Numerical data analytics (traffic, cpu, …)
- **Syslog analytics**
- Trouble tickets analytics
- Workflow analytics
- Twitter analytics
- …

NTT

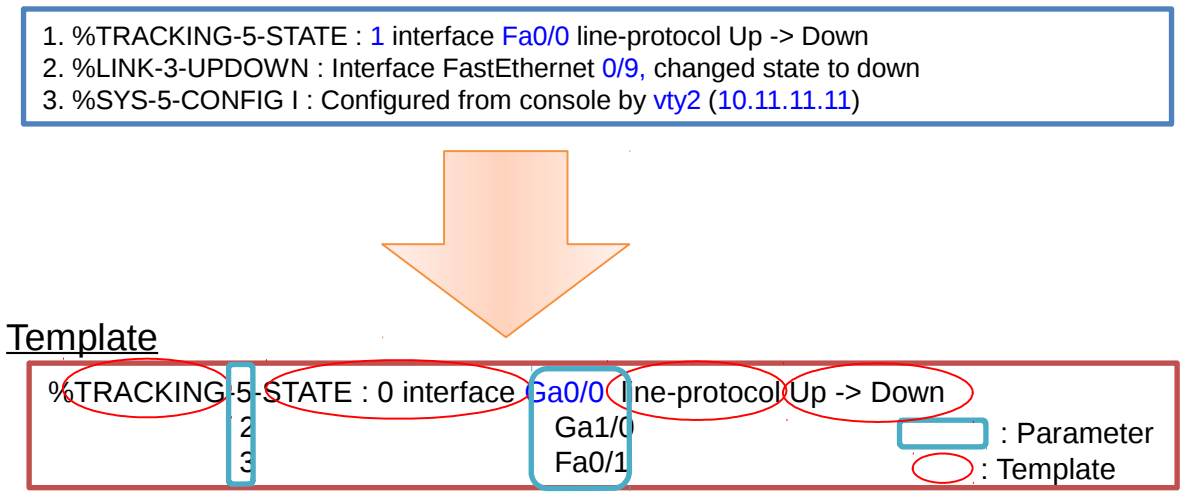
Syslog analytics: What is Syslog?

- Logging messages generated by a device (incl. server, router, s witch, …) to track software and hardware conditions.
  - Intended for debugging software and hardware problem of device.
- Free-form texts
  - Syntax and semantics are different among device vendors and operat ing systems.
- Huge amount data generated.



Syslog analytics: Issue1
Template identification

- Free-form texts is used for detailed information.
  - Syntax and semantics varies among device vendors and operating systems.
- Identify template without prior knowledge on syntax and semantics.
  - Words of message is classified into keyword and parameter.



Syslog analytics: Idea1 Template identification

- Scoring frequency of words among similar messages
  - parameter words appear infrequently compared to template words in each position
- Clustering score, and determine parameter words for each message
  - thresholds for score of parameter words differ depending on log messages
  - density-based clustering algorithm (DBSCAN)

raw log messages:
<189> security telnet connection 15720 with 10.7.11.11 broken
<189> security telnet connection 18340 with 10.8.9.123 broken

1	2	3	4	5	6	7
<189>	security	telnet	15720	with	10.7.11.11	broken
<189>	security	telnet	18340	with	10.8.9.123	broken

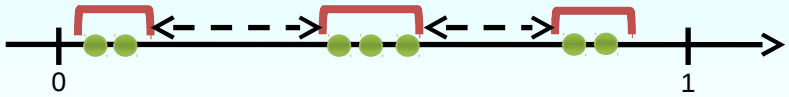
Remove

log template:
<189> security telnet connection * with * broken

Scoring:
If *word* appears in *P*-th position in log that contains *L* words:

$$Score(word, P, L) = \Pr(word \mid P, L)$$

Clustering scores (DBSCAN):
Distance between each cluster is > δ



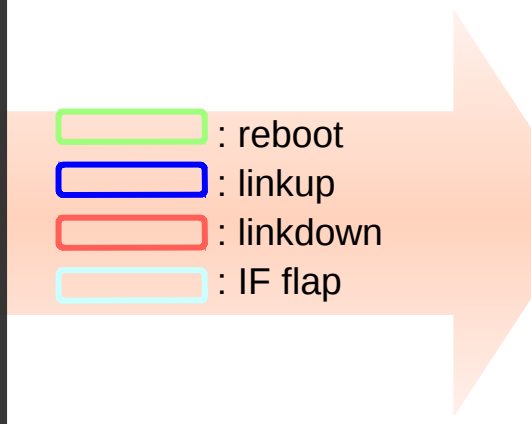
Syslog analytics: Issue2
Event identification

Innovative R&D by NTT

- Capture signature of co-occurred syslog m sgs.
- Associate a group of syslog msgs with an event of network.

Syslog

```
2012-1-1T00:00:00 %TRACKING-5-STATE: 1 interface Fa0/0 line-protocol Up->Down
2012-1-1T00:00:00 %LINK-3-UPDOWN: Interface FastEthernet 0/9, changed state to down
2012-1-1T00:00:00 %SYS-5-CONFIG I: Configured from console by vty2 (10.11.11.11)
2012-1-1T01:11:00 msg [100]:  STP: VLAN 1 Port 38 STP State -> DISABLED (PortDown)
2012-1-1T01:11:00 msg [101]: System: Interface ethernet 38, state down
2012-1-1T03:00:00 msg [200] : STP: VLAN 100 Port 22 STP State -> DISABLED (PortDown)
2012-1-1T03:00:00 msg [201] : System: Interface ethernet 22, state down
2012-1-1T00:00:00 %SYS-5-CONFIG I: Configured from console by vty2 (10.11.11.11)
2012-1-1T10:30:00 System: Interface ethernet 1, state down
2012-1-1T10:30:00 System: Interface ethernet 1, state up
2012-1-1T10:30:00 System: Interface ethernet 2, state down
2012-1-1T12:00:00 init: alarm-control (PID 111) terminate signal sent
2012-1-1T12:00:00 init: bslockd (PID 124 ) terminate signal sent
2012-1-1T12:00:00 init: ce-l2tp-service (PID 123 ) terminate signal sent
2012-1-1T12:00:00 init: chassis-control (PID 1111 ) terminate signal sent
2012-1-1T12:00:00 init: class-of-service (PID 11112)  terminate signal sent
2012-1-1T12:00:00 init: craft-control (PID 111) terminate signal sent
2012-1-1T12:00:00 init: database-replication (PID 2718932 ) terminate signal sent
2012-1-1T12:00:00 init: diameter-service (PID 2993 ) terminate signal sent
2012-1-1T12:00:00 init: disk-monitoring (PID 7082 ) terminate signal sent
2012-1-1T00:00:00 %SYS-5-CONFIG I: Configured from console by vty2 (10.11.11.11)
2012-1-1T15:45:10 msg [200] : STP: VLAN 100 Port 22 STP State -> DISABLED (PortDown)
2012-1-1T15:45:10 msg [201] : System: Interface ethernet 22, state down
2012-1-1T16:12:40 System: Interface ethernet 1, state down
2012-1-1T16:12:40 System: Interface ethernet 1, state up
2012-1-1T16:12:40 System: Interface ethernet 2, state down
2012-1-1T20:30:00 init: alarm-control (PID 111) terminate signal sent
2012-1-1T20:30:00 init: bslockd (PID 124 ) terminate signal sent
2012-1-1T20:30:00 init: ce-l2tp-service (PID 123 ) terminate signal sent
2012-1-1T20:30:00 init: chassis-control (PID 1111 ) terminate signal sent
2012-1-1T20:30:00 init: class-of-service (PID 11112)  terminate signal sent
```

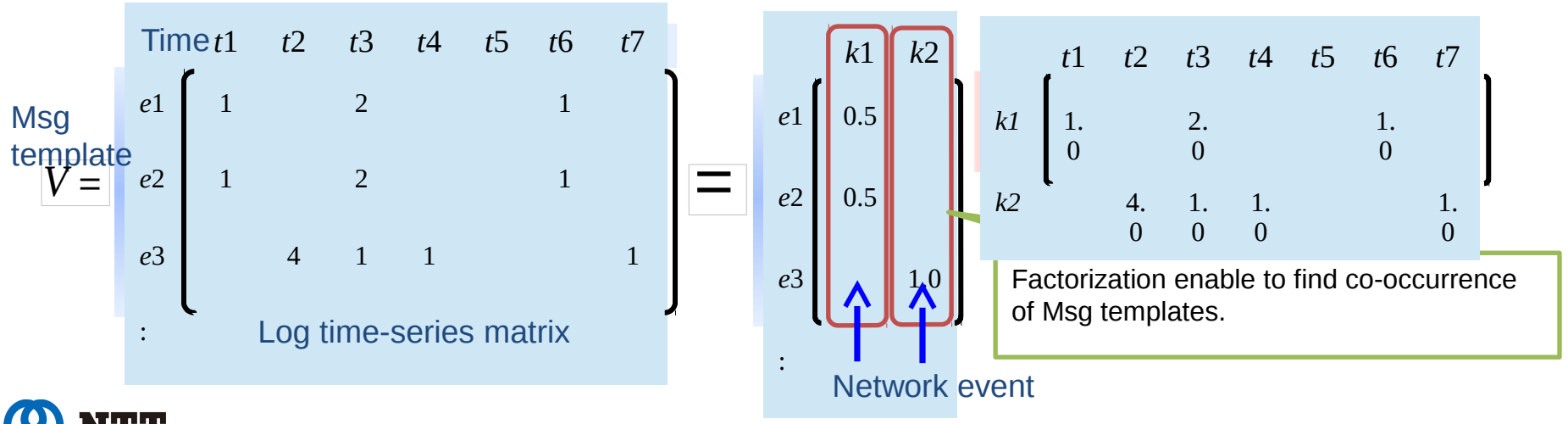


Associate network event
(Exploit Co-occurrence)

```
2012-1-1T00:00:00 %TRACKING-5-STATE: 1 interface Fa0/0 line-protocol Up->Down
2012-1-1T00:00:00 %LINK-3-UPDOWN: Interface FastEthernet 0/9, changed state to down
2012-1-1T00:00:00 %SYS-5-CONFIG I: Configured from console by vty2 (10.11.11.11)
2012-1-1T01:11:00 msg [100]:  STP: VLAN 1 Port 38 STP State -> DISABLED (PortDown)
2012-1-1T01:11:00 msg [101]: System: Interface ethernet 38, state down
2012-1-1T03:00:00 msg [200] : STP: VLAN 100 Port 22 STP State -> DISABLED (PortDown)
2012-1-1T03:00:00 msg [201] : System: Interface ethernet 22, state down
2012-1-1T00:00:00 %SYS-5-CONFIG I: Configured from console by vty2 (10.11.11.11)
2012-1-1T10:30:00 System: Interface ethernet 1, state down
2012-1-1T10:30:00 System: Interface ethernet 1, state up
2012-1-1T10:30:00 System: Interface ethernet 2, state down
2012-1-1T12:00:00 init: alarm-control (PID 111) terminate signal sent
2012-1-1T12:00:00 init: bslockd (PID 124 ) terminate signal sent
2012-1-1T12:00:00 init: ce-l2tp-service (PID 123 ) terminate signal sent
2012-1-1T12:00:00 init: chassis-control (PID 1111 ) terminate signal sent
2012-1-1T12:00:00 init: class-of-service (PID 11112)  terminate signal sent
2012-1-1T12:00:00 init: craft-control (PID 111) terminate signal sent
2012-1-1T12:00:00 init: database-replication (PID 2718932 ) terminate signal sent
2012-1-1T12:00:00 init: diameter-service (PID 2993 ) terminate signal sent
2012-1-1T12:00:00 init: disk-monitoring (PID 7082 ) terminate signal sent
2012-1-1T00:00:00 %SYS-5-CONFIG I: Configured from console by vty2 (10.11.11.11)
2012-1-1T15:45:10 msg [200] : STP: VLAN 100 Port 22 STP State -> DISABLED (PortDown)
2012-1-1T15:45:10 msg [201] : System: Interface ethernet 22, state down
2012-1-1T16:12:40 System: Interface ethernet 1, state down
2012-1-1T16:12:40 System: Interface ethernet 1, state up
2012-1-1T16:12:40 System: Interface ethernet 2, state down
2012-1-1T20:30:00 init: alarm-control (PID 111) terminate signal sent
2012-1-1T20:30:00 init: bslockd (PID 124 ) terminate signal sent
2012-1-1T20:30:00 init: ce-l2tp-service (PID 123 ) terminate signal sent
2012-1-1T20:30:00 init: chassis-control (PID 1111 ) terminate signal sent
2012-1-1T20:30:00 init: class-of-service (PID 11112)  terminate signal sent
```

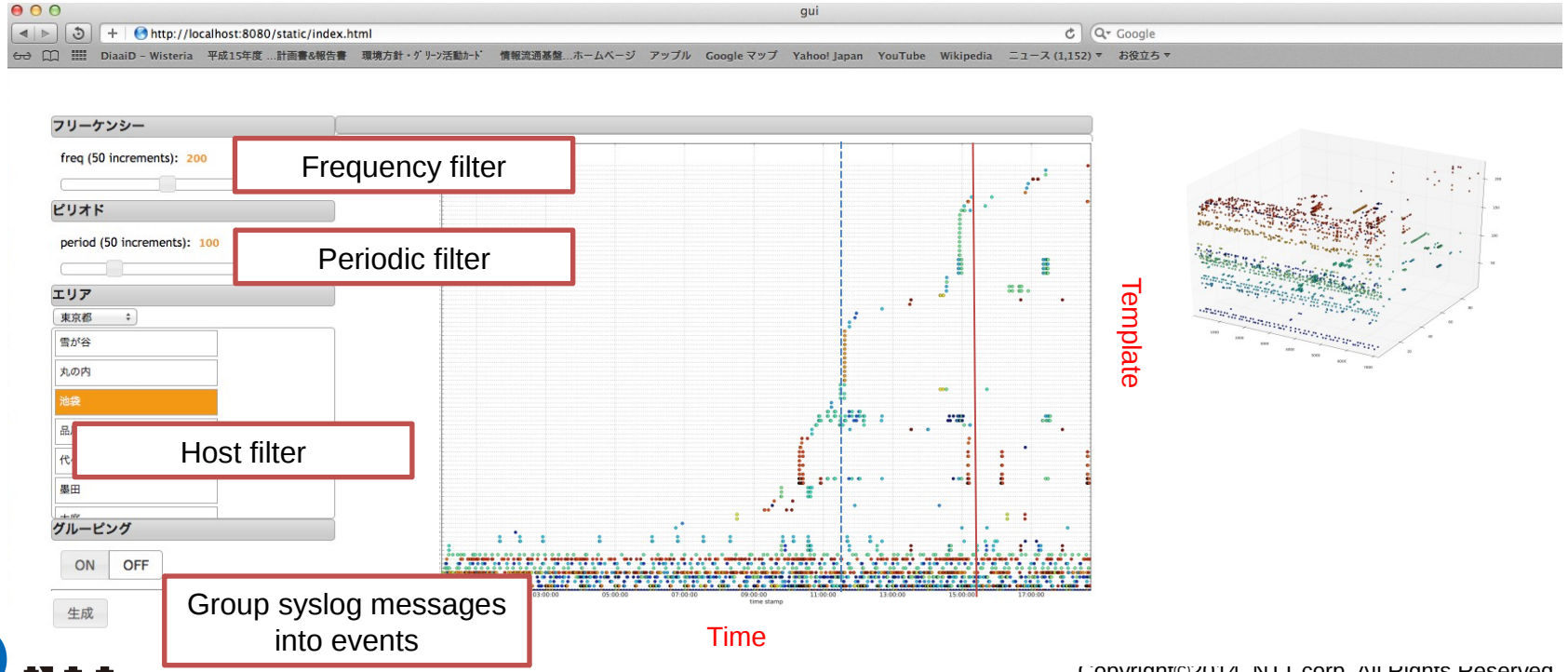
Syslog analytics: Idea2 NMF and NTF

- Non-negative matrix/tensor factorization
  - Time-series data of syslog messages are expressed in matrix/tensor form.
  - Matrix/tensor is factorized.
    - Time-series data is considered as a mixture of different network events occurred in the network.
    - Network event is extracted as a combination of templates.



Syslog analytics: visualization

- Visualize massive time-series syslog data for easy understanding.
- Apply frequency & periodic filters to remove unimportant messages.
- Group syslog messages into events.



(2) Robust traffic engineering

Robust traffic engineering

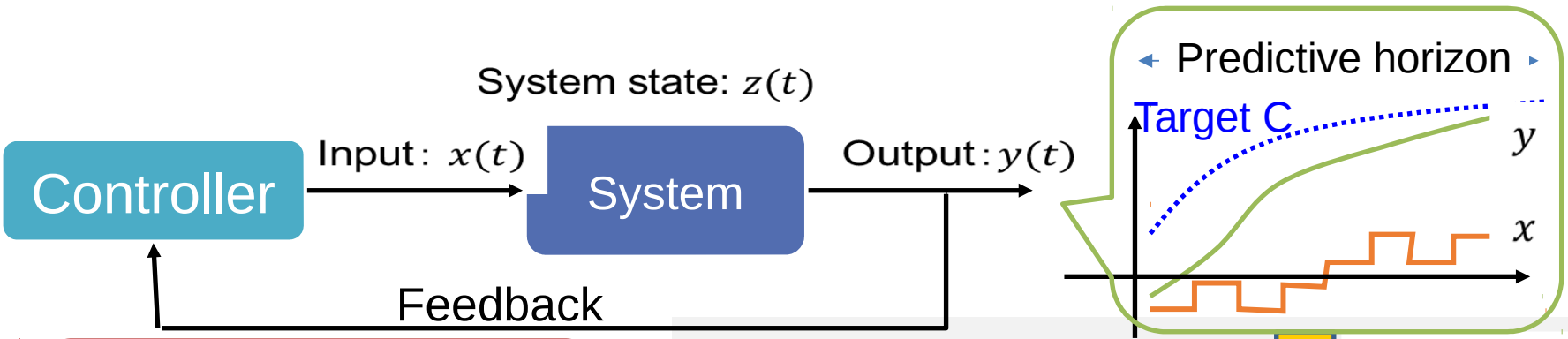
Innovative R&D by NTT

Actuate the network based on the decision

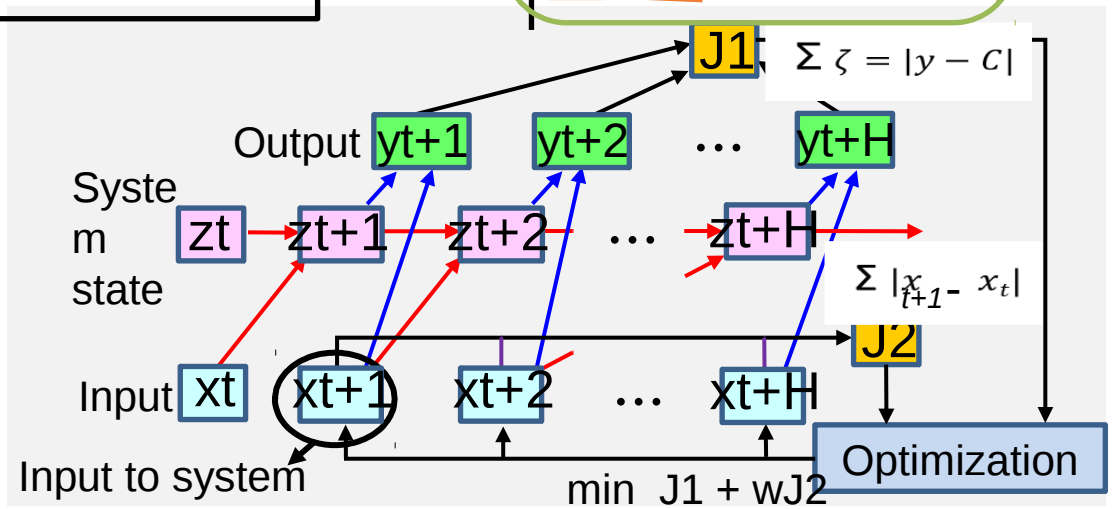
- Robust to prediction error

Model Predictive Control (MPC)

- Predict the process output at future time instants (***horizon***).
- Calculate a control sequence in the horizon to optimize an objective function.
- Only the first step of the control sequence is applied in a receding strategy, where at each inst ant the horizon is displaced towards the future.

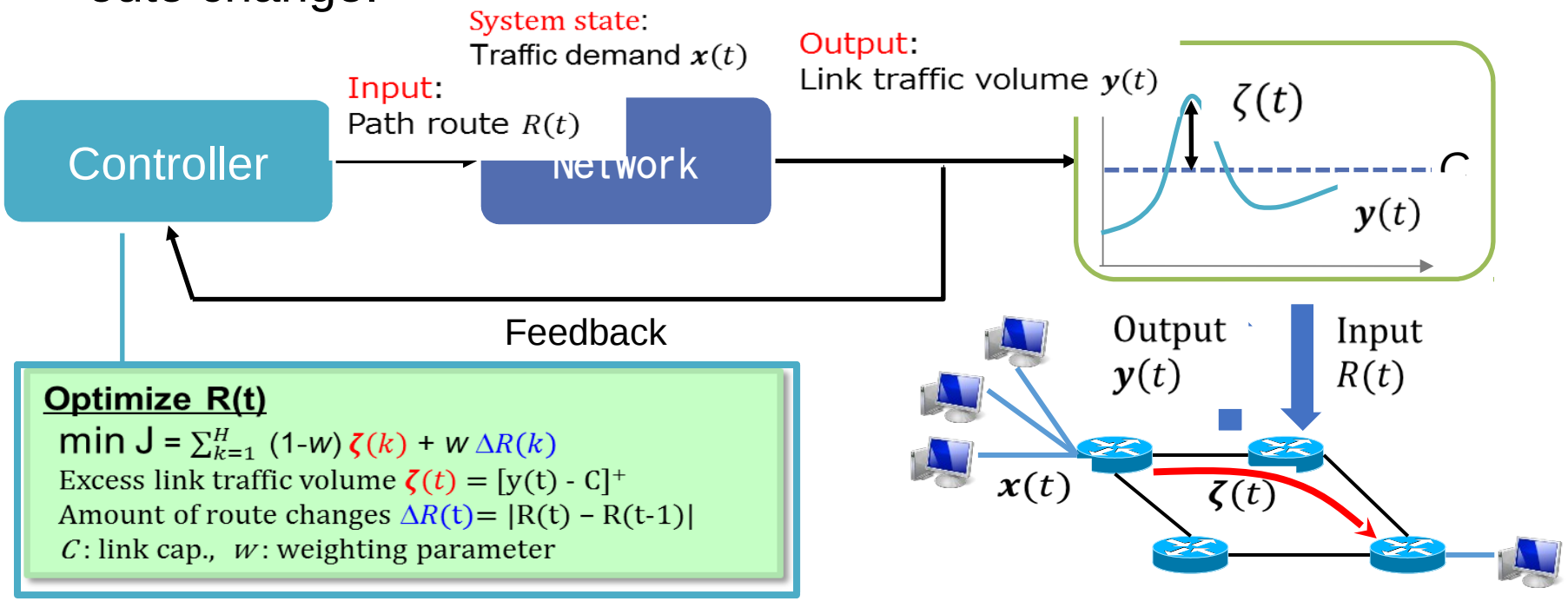


Reduces amount of change in x(t) to sustain stability of system and improve robustness against estimation error



Application of MPC to TE

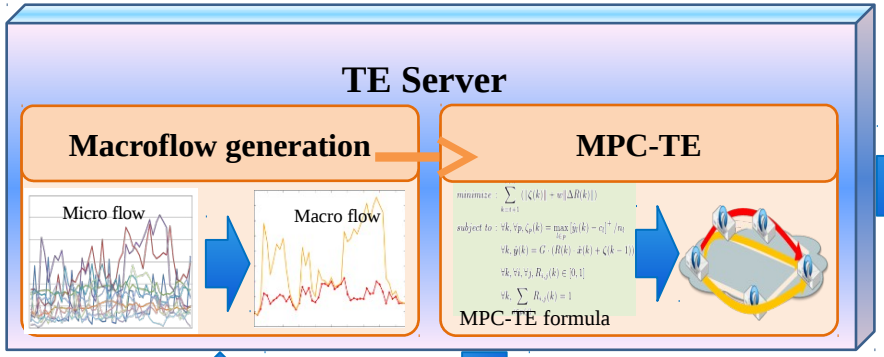
- Path routes are computed for several time epochs in the future (horizon).
- Objective is to reduce the excess bandwidth and the amount of r oute change.

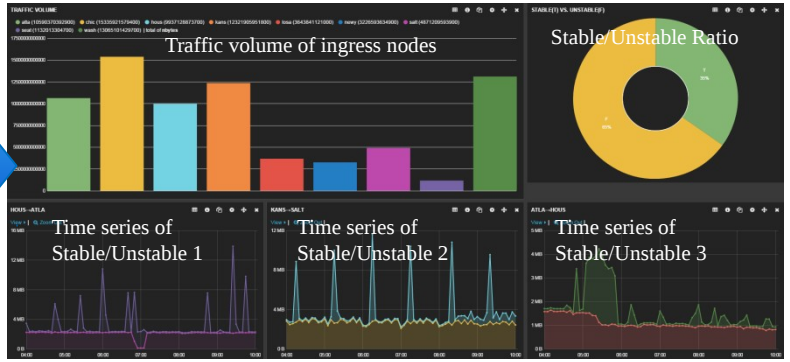


Proof-of-concept

Innovative R&D by NTT

Internet2: packet capture data & topology

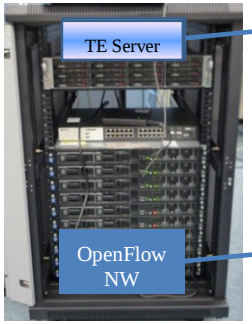




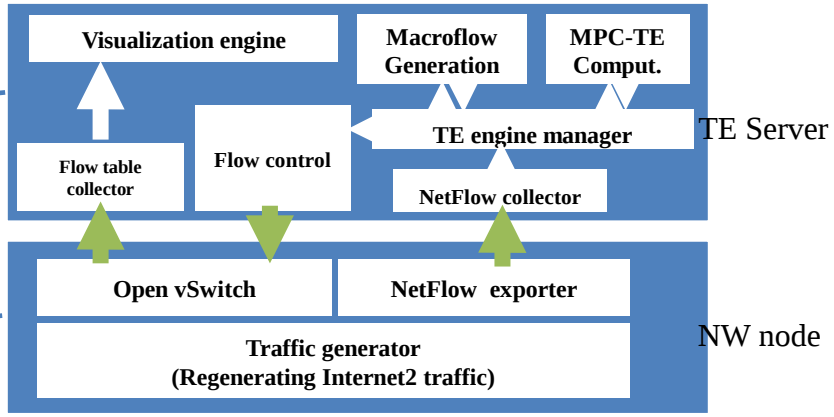
Flow collection (200k records/min)

5 min cycle

Route change (1000 entries/switch)



PoC system



Module component

Thank you for your attention