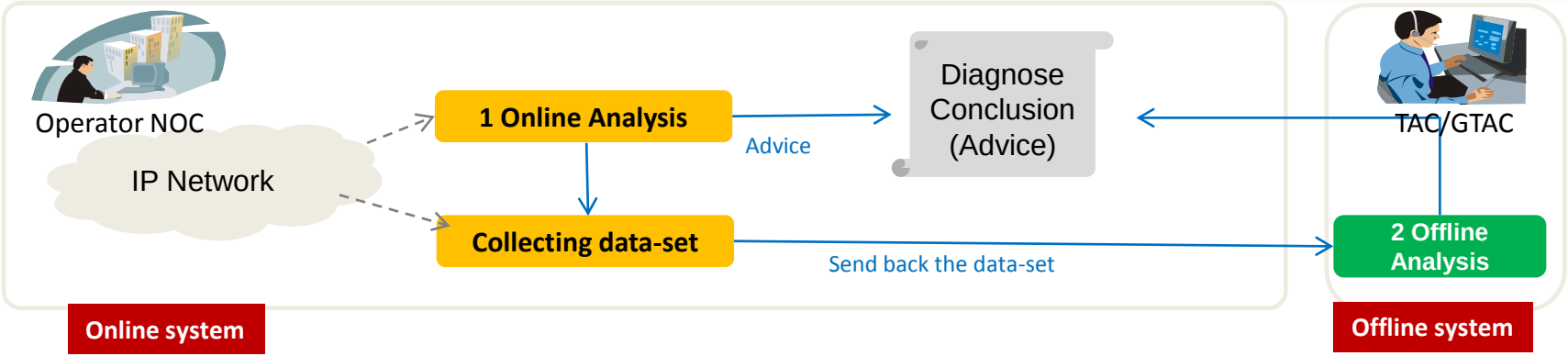
Research on Network Fault Analysis based on Machine Learning

Haibin Song (speaker), (haibin.song@huawei.com)
Liang Zhang (zhangliang1@huawei.com)

HUAWEI TECHNOLOGIES CO., LTD.

Example Scenario of Big data analysis

- **Goal：Combine the offline and online analysis system to support the fast recovery of fault**
- **Online Analysis：** Deployed in customer side, detect the fault at real-time, could give out the advice
- **Offline Analysis：** Deployed in TAC/GTAC, provide the service for the global customs, help engineer to locate the fault and give the advice



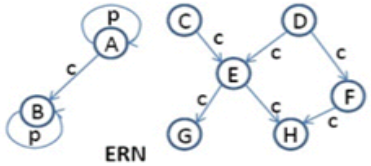
No	System	User	Feature
1	Online Analysis	Customer	❑ Proactive monitoring of the state of functioning and health of telecommunication equipment ❑ The detection of the earliest symptoms of a malfunction for network devices ❑ Correlation analysis on the basis of the multiple data sets
2	Offline Analysis	TAC/GTAC	❑ Data Visualization to help user get the insight to the fault. ❑ The detection of the fault of a malfunction for network devices ❑ Correlation analysis on the basis of the multiple data sets

Offline Scenario for Fault Analysis

Data upload

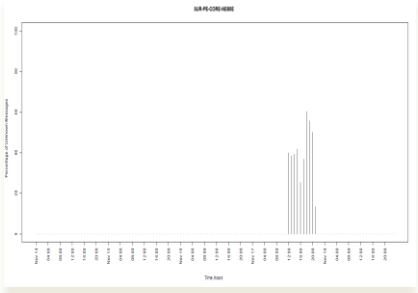
Automatic Fault Analysis

Visualization



KPI Analysis

Anomaly analysis



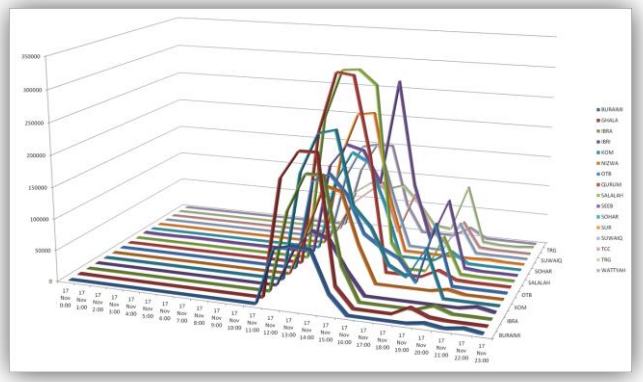
Correlation analysis

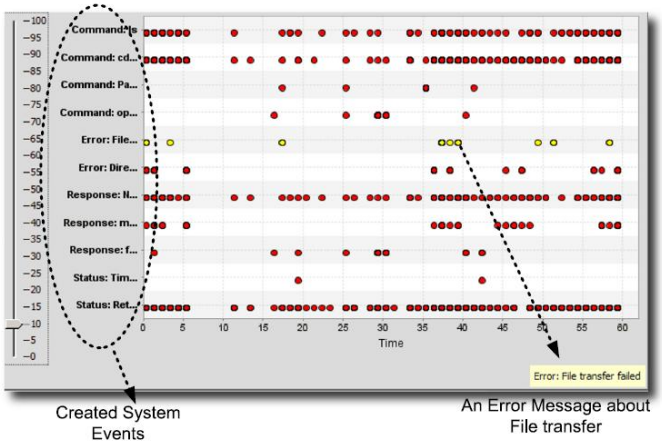
items	support
1 {BFD BFD_DOWN_TRAP , BFD CRTSESS , BFD DELSESS , BFD STACHG_TODWN , BFD STACHG_TOUP , OSPF NBRCHG , OSPF NBR_CHANGE_E , OSPF NBR_CHG_DOWN , OSPF NBR_DOWN_REASON , OSPF OGNLSA }	0.2523030

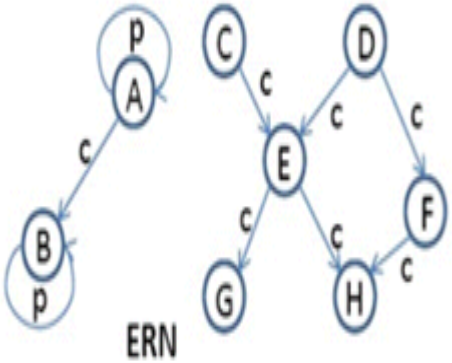
Visualization——Get the insight to fault

Value

1 Filter unnecessary information
2 Statistical analysis of events



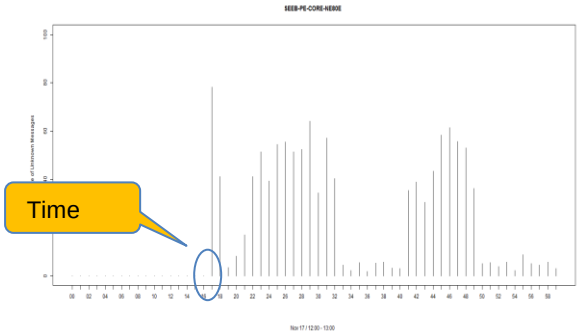


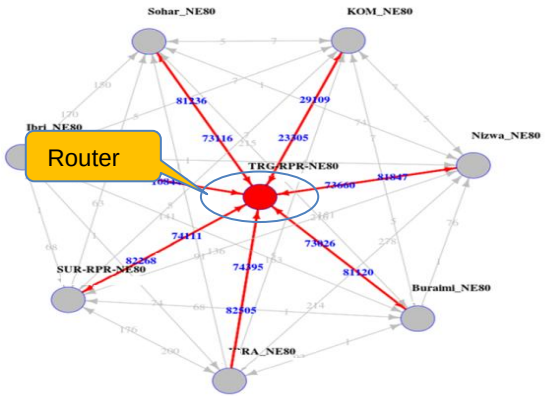


Anomaly Detection

Value

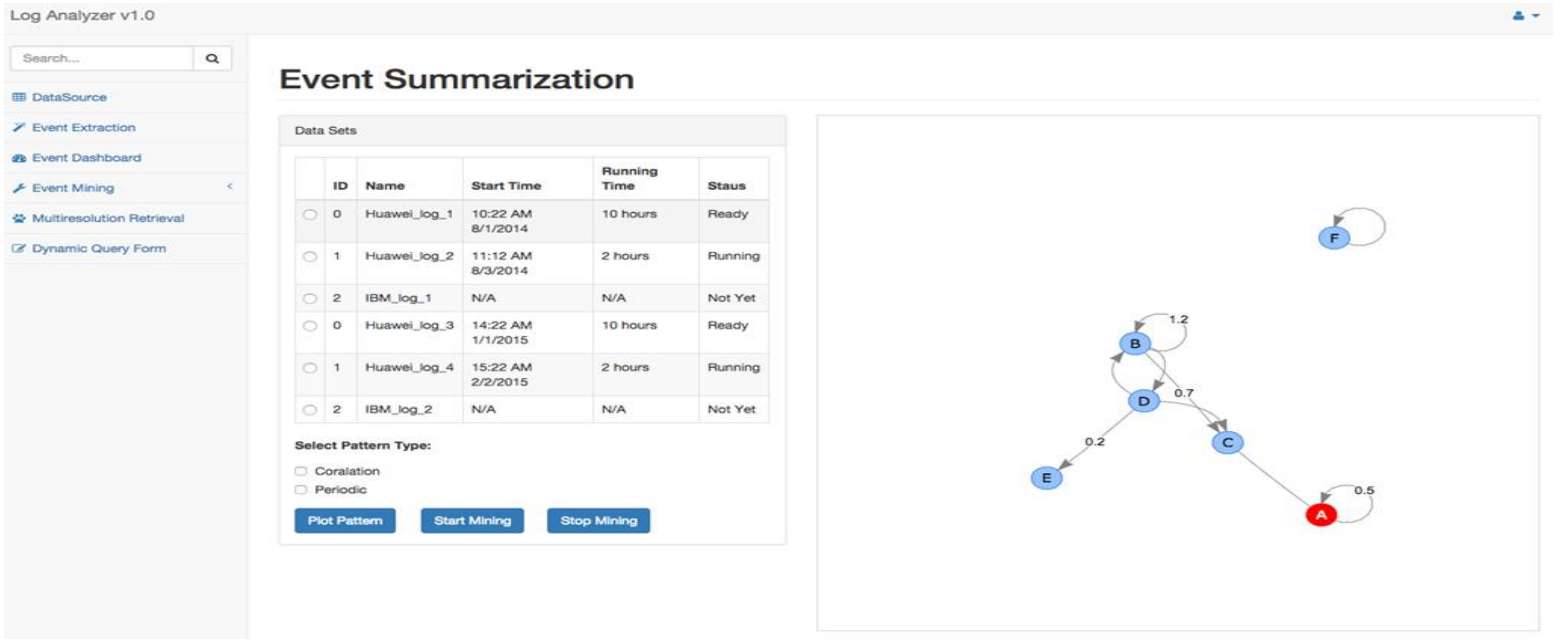
1 Find the possible fault time
2 Find the possible device
3 Find the possible module





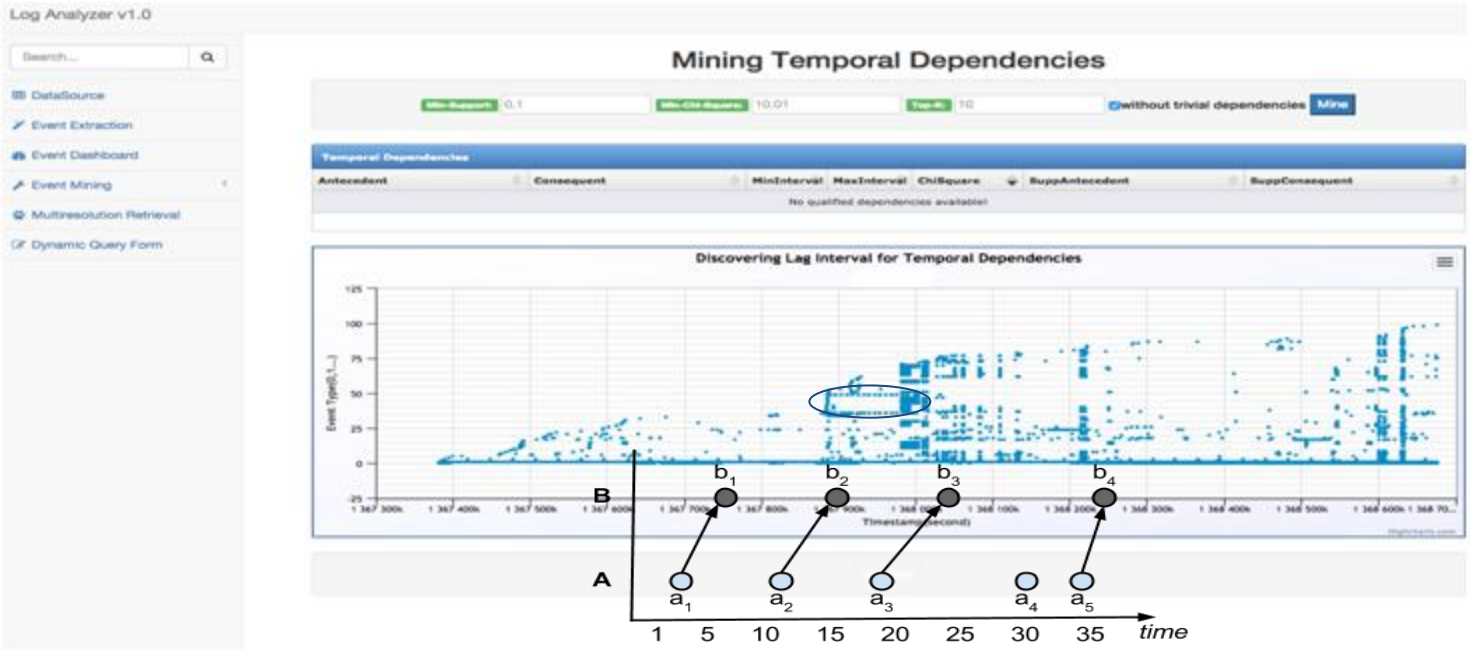
- Related log files
- 17:20 shutdown Cmd

Visualization—Event Summarization



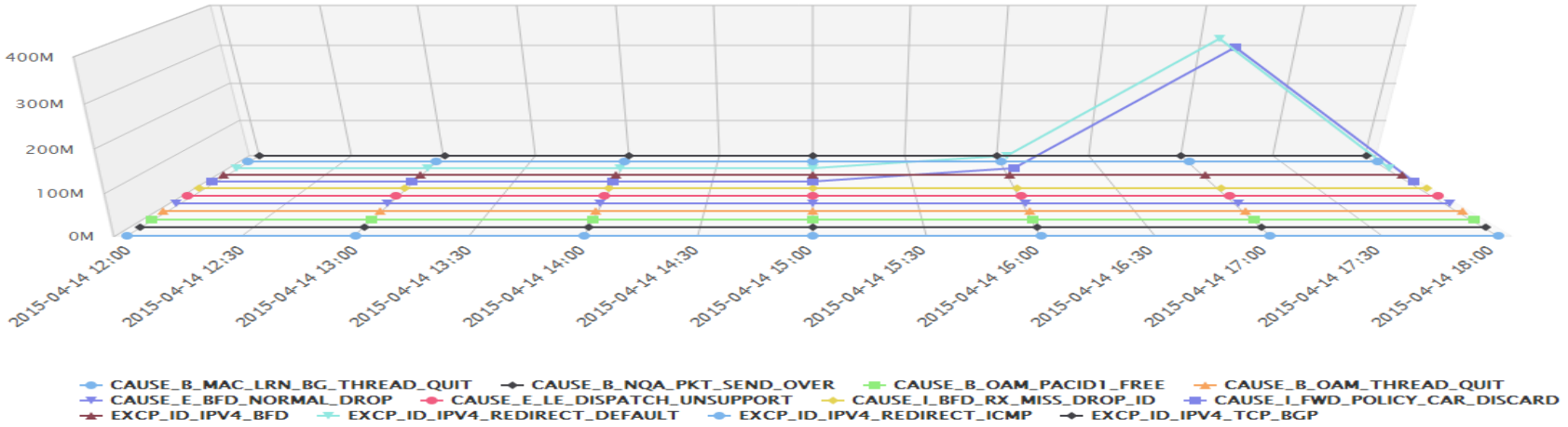
- Get the event summarization between different events, and find the relationship between them.

Visualization—— Lag interval



- Time lag is a key feature of hidden temporal dependencies within sequential data.

Anomaly Detection——KPI



分析结果

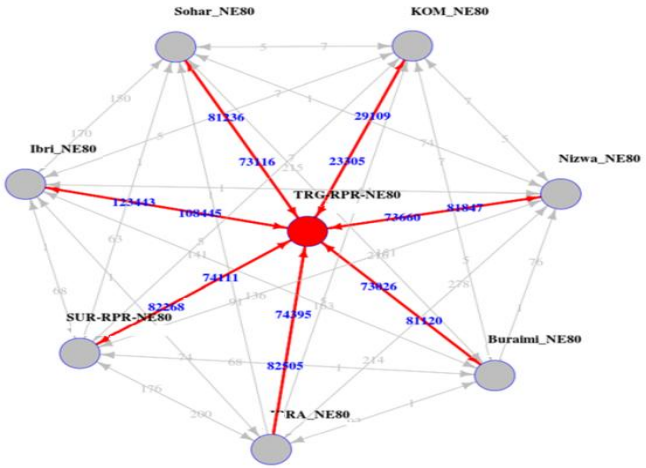
上一页 下一页 到第 1 页 共 1 页(每页 5 条)

异常时间	设备	槽位	异常ID	丢包数量/分钟
2015-04-14 16:56:00	79-4-8-Floor-HW-PTN2	1	CAUSE_I_FWD_POLICY_CAR_DISCARD	10256137
			EXCP_ID_IPV4_REDIRECT_ICMP	10255106
			EXCP_ID_IPV4_REDIRECT_DEFAULT	4
			EXCP_ID_IPV4_TCP_BGP	21

- **Help the operators find the root cause KPI among a list of KPIs, and find the fault time.**

Anomaly Detection——Multiple log files

	row.names	KOM_NE80	TRG-RPR-NE80	Buraimi_NE80	IBRA_NE80	Ibri_NE80	Nizwa_NE80	Sohar_NE80	SUR-RPR-NE80
1	KOM_NE80	0	23305	5	5	5	5	5	5
2	TRG-RPR-NE80	29109	0	81120	82505	123443	81847	81236	82268
3	Buraimi_NE80	7	73826	0	92	141	76	215	68
4	IBRA_NE80	7	74395	1	0	1	278	1	176
5	Ibri_NE80	7	108445	163	74	0	64	150	68
6	Nizwa_NE80	7	73660	1	214	1	0	1	136
7	Sohar_NE80	7	73116	216	91	170	74	0	63
8	SUR-RPR-NE80	7	74111	1	200	1	151	1	0



KOM_NE80\0.1243918 TRG-RPR-NE80\1.0000000 Buraimi_NE80\0.3666137 IBRA_NE80\0.3731849
Ibri_NE80\0.5507581 Nizwa_NE80\0.3697645 Sohar_NE80\0.3671156 SUR-RPR-NE80\0.3717175

Interaction frequency matrix for ISIS protocol messages

Output of the Rage Rank algorithm

- **Find the root cause router based on the interaction of the protocol**

Thank you

Comments?