PreFix: Switch Failure Prediction in Datacenter Networks

Sen Yang

Joint work with
Shenglin Zhang, Ying Liu, Weibin Meng, Zhiling Luo, Jiahao Bu, Peixian Liang, Dan Pei, Jun Xu, Yuzhi Zhang, Yu Chen, Hui Dong, Xianping Qu, Lei Song

Nankai University, 1
Peking University, 2
Xi’an Jiaotong University, 3
Georgia Tech, 4
Notre Dame, 5
Baidu, 6

2018/6/21 SIGMETRICS 2018
Network Devices in Data Center Networks

Inter-DC Network

ToR Switch

Server

Aggregation Switch

ToR Switch

Access Router

Firewall

IDPS

VPN

Load balancer

L2

L3

Core Router

Firewall

IDPS

VPN

Load balancer

SIGMETRICS 2018
Network Devices in Data Center Networks

- **Switch**
  - Top-of-rack switch
  - Aggregation switch

- **Router**
  - Access router
  - Core router

- **Middle box**
  - Firewall
  - Intrusion detection and prevention system (IDPS)
  - Load balancer
  - VPN
Network Devices in Data Center Networks

- **Switch**
  - Top-of-rack switch
  - Aggregation switch

- **Router**
  - Access router
  - Core router

- **Middle box**
  - Firewall
  - Intrusion detection and prevention system (IDPS)
  - Load balancer
  - VPN
Scale of Network Devices in Datacenter

- Hundreds of thousands to millions of servers
- Hundreds of thousands of switches
- Millions of cables and fibers

Microsoft (C. Guo, et al., SIGCOMM'15)
Scale of Network Devices in Datacenter

- Microsoft (C. Guo, et al., SIGCOMM'15)
  - Hundreds of thousands to millions of servers
  - Hundreds of thousands of switches
  - Millions of cables and fibers

- Baidu
  - Hundreds of thousands of servers
  - Tens of thousands of switches
Scale of Network Devices in Datacenter

- **Microsoft (C. Guo, et al., SIGCOMM’15)**
  - Hundreds of thousands to millions of servers
  - Hundreds of thousands of switches
  - Millions of cables and fibers

- **Baidu**
  - Hundreds of thousands of servers
  - Tens of thousands of switches

- **Switch failures are the norm rather than the exception (P. Gill, et al., SIGCOMM’11)**
  - More than 400 switch failures per year
Switch Failures Lead to Outages

- A Cisco switch failure at the datacenter of Hosting.com
- Affected a number of services including AWS for 1.5 hours
A Cisco switch failure at the datacenter of Hosting.com
- Affected a number of services including AWS for 1.5 hours

The datacenter network went dark after a switch failure
- Almost every executive branch agency are affected for a few hours
Switch Failure

• “An event that occurs when the switch is not functioning for forwarding traffic” [1]

Switch Failure

Observable[1]

- A human
- A server
- Another network device
- If not result in incorrect output, it is not a failure

Switch Failure

Observable[1]
- A human
- A server
- Another network device
- If not result in incorrect output, it is not a failure

Failure tickets
- Regular expression match with syslogs
- Feedback by Internet services
- Monitoring results of interfaces

Previous Proposed Solutions

Change the protocols and network topologies

• Aim to automatically failover
• ToR switches do not have hot backups
Previous Proposed Solutions

Change the protocols and network topologies

• Aim to automatically failover
• ToR switches do not have hot backups

Locate and diagnose failed switches

• Face deployment challenges
• Take time to locate and fix the failed switches
• Drop packets silently and affect services

Failure Prediction for Switches

- During runtime
- Near future
- Based on the monitored current switch state
- Mining historical failure cases of switches
Failure Prediction for Switches Based on Syslogs

• Sep  8 15:44:30 192.168.191.85 192.168.191.85 : [SIF]Interface ae3, changed state to down
• Sep  8 15:45:51 192.168.191.85 192.168.191.85 : [SIF]Vlan-interface vlan22, changed state to down
• Sep  8 15:46:59 192.168.191.85 192.168.191.85 : [SIF]Interface ae3, changed state to up
• Sep  8 15:47:21 192.168.191.85 192.168.191.85 : [SIF]Vlan-interface vlan22, changed state to up
• Sep  8 15:48:30 192.168.191.85 192.168.191.85 : [OSPF]Neighbour(rid:10.231.0.42, addr:10.231.38.85) on vlan22, changed state from Full to Down
• Sep  8 15:49:35 192.168.191.85 192.168.191.85 : [SIF]Interface ae3, changed state to down
• Sep  8 15:49:45 192.168.191.85 192.168.191.85 : [SIF]Vlan-interface vlan22, changed state to down
• Sep  8 15:50:42 192.168.191.85 192.168.191.85 : [SIF]Interface ae3, changed state to up
• Sep  8 15:50:59 192.168.191.85 192.168.191.85 : [SIF]Vlan-interface vlan22, changed state to up
• Sep  8 15:51:22 192.168.191.85 192.168.191.85 : [OSPF]A single neighbour should be configured
• Sep  8 15:51:52 192.168.191.85 192.168.191.85 : [OSPF]A single neighbour should be configured
• Sep  8 15:52:46 192.168.191.85 192.168.191.85 : [SIF]Interface ae1, changed state to down
• Sep  8 15:53:24 192.168.191.85 192.168.191.85 : [SIF]Vlan-interface vlan20, changed state to down
• Sep  8 15:54:31 192.168.191.85 192.168.191.85 : [OSPF]Neighbour(rid:10.231.0.40, addr:10.231.36.85) on vlan20, changed state from Full to Down
• Sep  8 15:55:12 192.168.191.85 192.168.191.85 : [SIF]Interface ae1, changed state to up
• Sep  8 15:56:47 192.168.191.85 192.168.191.85 : [SIF]Vlan-interface vlan20, changed state to up
• Sep  8 15:59:01 192.168.191.85 192.168.191.85 : [OSPF]A single neighbour should be configured

• Sep  8 16:31:20 whole machine failure (labelled by the operators)
### Challenges

**Noisy signals in syslog data**

- Syslogs are highly diverse
  - Across several geographical locations, network layers, protocols, services
- Normal login events of operators
- Interface up/downs
- Failure to send/receive packets
- Rarely contain failure omens
Challenges

Noisy signals in syslog data

• Syslogs are highly diverse
• Across several geographical locations, network layers, protocols, services
• Normal login events of operators
• Interface up/downs
• Failure to send/receive packets
• Rarely contain failure omens

Sample imbalance

• Low failure possibility for a single switch
• Failure omen time bins: failure non-omen time bins = 1:72500
• Low false alarms and high recall at the same time
Design Overview

Offline Learning Component
- Historical Syslogs
- Template Learning
- Template Matching
- Feature Extraction (Frequency, Surge, Seasonality, Sequence)
- LCS Set $\Omega$
- Training using RF
- Operations team
- Parameters
- Failures
- Online Failure Prediction

Online Prediction Component
- Realtime Syslogs
- Template Matching
- Template Matching
- Feature Extraction (Frequency, Surge, Sequence)
- Online Failure Prediction

Template

Templates
Design Overview

Offline Learning Component

Online Prediction Component

Historical Syslogs

Template Learning

Template Matching

Templates

Feature Extraction

Frequency

Surge

Seasonality

Sequence

$LCS$ Set $\Omega$

Operations team

Training using RF

Parameters

Failures

Realtime Syslogs

Template Matching

Templates

Feature Extraction

Sequence

Surge

Feature Extraction

Online Failure Prediction
Design Overview

Realtime Syslogs → Template Learning

Historical Syslogs → Template Matching

Templates → LCS Set Ω

Feature Extraction:
- Frequency
- Surge
- Seasonality
- Sequence

Operations team:
- Training using RF
- Parameters

Failures → Online Prediction Component

Template Matching:
- Sequence
- Feature Extraction

Online Failure Prediction

Realtime Syslogs → Template Matching
Design Overview

Design Overview

Offline Learning Component
- Training using RF
  - Parameters
    - Failures
  - Operations team

Online Prediction Component
- Online Failure Prediction
- Feature Extraction
  - Frequency
  - Surge
  - Seasonality
  - Sequence
- Template Matching
  - Templates
  - LCS Set $\Omega$

Realtime Syslogs
- Template Learning
  - Templates
- Template Matching

Historical Syslogs
- Template Learning
  - Templates
  - Template Matching
Several failures share common syslog sequences
Several failures share common syslog sequences

Some syslogs are indicative of failures when they occur in a sudden burst
E.g., interface up/down
Several failures share common syslog sequences

Some syslogs are indicative of failures when they occur in a sudden burst
E.g., interface up/down

Frequent syslogs can be ignored
E.g., package loss ratio of PING sessions
Several failures share common syslog sequences

Some syslogs are indicative of failures when they occur in a sudden burst
E.g., interface up/down

Frequent syslogs can be ignored
E.g., package loss ratio of PING sessions

Some syslogs are periodic and irrelevant to failures
E.g., daily maintenance operations
Several failures share common syslog sequences

Some syslogs are indicative of failures when they occur in a sudden burst
E.g., interface up/down

Frequent syslogs can be ignored
E.g., package loss ratio of PING session

Some syslogs are periodic and irrelevant to failures
E.g., daily maintenance operations
Several failures share common syslog sequences.

**Surge**

Some syslogs are indicative of failures when they occur in a sudden burst.
E.g., interface up/down

**Frequency**

Frequent syslogs can be ignored.
E.g., package loss ratio of PING session

**Seasonality**

Some syslogs are periodic and irrelevant to failures.
E.g., daily maintenance operations
Several failures share common syslog sequences

Some syslogs are indicative of failures when they occur in a sudden burst
E.g., interface up/down

Frequent syslogs can be ignored
E.g., package loss ratio of PING session

Some syslogs are periodic and irrelevant to failures
E.g., daily maintenance operations
Several failures share common syslog sequences

Some syslogs are indicative of failures when they occur in a sudden burst
E.g., interface up/down

Frequent syslogs can be ignored
E.g., package loss ratio of PING session

Some syslogs are periodic and irrelevant to failures
E.g., daily maintenance operations

Feature Extraction

Sequence
Surge
Frequency
Seasonality

Sample imbalance

Failure omens
Non-failure omens
Syslogs Before a Failure (Within 2 Hours)

- Sep 8 15:44:30 192.168.191.85 192.168.191.85: [SIF] Interface ae3, changed state to down
- Sep 8 15:45:51 192.168.191.85 192.168.191.85: [SIF] Vlan-interface vlan22, changed state to down
- Sep 8 15:46:59 192.168.191.85 192.168.191.85: [SIF] Interface ae3, changed state to up
- Sep 8 15:48:30 192.168.191.85 192.168.191.85: [OSPF] Neighbour (rid:10.231.0.42, addr:10.231.38.85) on vlan22, changed state from Full to Down
- Sep 8 15:49:35 192.168.191.85 192.168.191.85: [SIF] Interface ae3, changed state to down
- Sep 8 15:50:42 192.168.191.85 192.168.191.85: [SIF] Interface ae3, changed state to up
- Sep 8 15:51:22 192.168.191.85 192.168.191.85: [OSPF] A single neighbour should be configured
- Sep 8 15:51:52 192.168.191.85 192.168.191.85: [OSPF] A single neighbour should be configured
- Sep 8 15:52:46 192.168.191.85 192.168.191.85: [SIF] Interface ae1, changed state to down
- Sep 8 15:54:31 192.168.191.85 192.168.191.85: [OSPF] Neighbour (rid:10.231.0.40, addr:10.231.36.85) on vlan20, changed state from Full to Down
- Sep 8 15:55:12 192.168.191.85 192.168.191.85: [SIF] Interface ae1, changed state to up
- Sep 8 15:59:01 192.168.191.85 192.168.191.85: [OSPF] A single neighbour should be configured
- Sep 8 16:31:20 whole machine failure (labelled by the operators)
Transfer to Template Tag Sequence

• The syslogs before failure 1 (2h)
  • 48 49 46 47 63 48 49 46 47 62 62 48 49 63 46 47 62
Transfer to Template Tag Sequence

• The syslogs before failure 1 (2h)
  • 48 49 46 47 63 48 49 46 47 62 62 48 49 63 46 47 62

• The syslogs before failure 2 (2h)
Transfer to Template Tag Sequence

• The syslogs before failure 1 (2h)
  • 48 49 46 47 63 48 49 46 47 62 62 48 49 63 46 47 62

• The syslogs before failure 2 (2h)
  • 0 48 48 48 48 46 46 46 46 46 46 48 48 46 46 48 48 46 46 48 46 46 48 48 46 46 48 49 63 51 50 46 47 62 48 48 46 46 51 50 51 50 48 49 48 49 63 51 46 47 50 63 46 47 48 49 62 62 46 47 62 48 49 46 47 62 48 49 63 51 50 46 47 62 56 57 58 59 44

• The syslogs before failure 3 (2h)
  • 48 48 49 49 63 63 46 46 47 47 62 62 56 56 57 57 58 58 59 59
Transfer to Template Tag Sequence

• The syslogs before failure 1 (2h)
  • 48 49 46 47 63 48 49 46 47 62 62 48 49 63 46 47 62

• The syslogs before failure 2 (2h)
  • 0 48 48 48 48 48 46 46 46 46 46 48 48 46 46 48 46 48 46 46 48 48 46 46 48 46 46
    48 46 48 49 63 51 50 46 47 62 48 48 46 46 51 50 51 50 48 49 48 49 63 51 46
    47 50 63 46 47 48 49 62 62 46 47 62 48 49 46 47 62 48 49 63 51 50 46 47 62
    56 57 58 59 44

• The syslogs before failure 3 (2h)
  • 48 48 49 63 63 46 46 47 47 62 62 56 56 57 57 58 58 59 59

• The syslogs before failure 4 (2h)
  • 51 50 48 49 63 46 47 62 48 49 46 47 62 51 51 50 50 50 51 50 48 49 63 51 46 47
    50 62 48 49 46 47 62 48 49 63 46 47 62 56 57 58 59 48 49 63 46 47 62 48 49
    46 47 48 49 63 51 46 47 50 62 62
Insights of the above examples

Syslogs before failures do share common subsequences

The sequence feature is helpful for predicting failures

Irrelevant syslogs (noises) exist before failures

Noise signals should be excluded
The LCS$^2$ method

- LCS$^2$
  - First step: filter noises and get longest common subsequences (LCSes)
  - Second step: measure the similarity
The LCS$^2$ method

- **LCS$^2$**
  - **First step:** filter noises and get longest common subsequences (LCSes)
  - **Second step:** measure the similarity

- **Filter noises and get LCSes**
  - Seq 1: 48 49 46 47 63 48 49 46 47 62 62 48 49 63 46 47 62
  - Seq 2: 48 48 49 49 63 63 46 46 47 47 62 62 56 56 57 57 58 58 58 59 59
  - Seq 3: 50 62 48 49 46 47 62 48 49 63 46 47 62 56 57 58 59 48 49 63 46 47 62 48 49 46 47 48 49 63 51 46 47 50 62 62
  - Seq 1 $\cap$ Seq 2: 48 48 49 49 63 46 47 62
  - Seq 1 $\cap$ Seq 3: 48 49 46 47 63 48 49 46 47 62 48 49 63 46 47 62
  - Seq 2 $\cap$ Seq 3: 48 48 49 49 63 46 46 47 47 62 62
The LCS\(^2\) method

- **LCS\(^2\)**
  - First step: filter noises and get longest common subsequences (LCSes)
  - Second step: measure the similarity

- **Measure the similarity**
  - Measure the similarity between current sequence and omen sequences
  - For each \(LCS_i\) in \(\Omega\)
    - \(LCS_{ci}\) is the LCS between the current sequence and \(LCS_i\)
    - Calculate the ratio of the length of \(LCS_{ci}\) to that of \(LCS_i, R_i\)
    - Apply \(\max(R_i)\) as the sequential feature score of the current sequence
The LCS$^2$ method

- **LCS$^2$**
  - First step: filter noises and get longest common subsequences (LCSes)
  - Second step: measure the similarity

- **Advantages**
  - Computationally efficient
  - Filter noises from failure omen sequences
Evaluation Experiments

- **Switches**
  - Three switch models
  - 9397 switches
  - 20+ data centers
  - 2-year period
- **Switch failures**
  - 415 switch failures
  - 1694 failure omen time bins
## Evaluation Experiments

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Method</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>PreFix</td>
<td>87.35%</td>
<td>74.36%</td>
<td>80.33%</td>
<td>$2.49 \times 10^{-5}$</td>
</tr>
<tr>
<td></td>
<td>SKSVM</td>
<td>8.25%</td>
<td>76.09%</td>
<td>14.89%</td>
<td>$1.96 \times 10^{-3}$</td>
</tr>
<tr>
<td></td>
<td>HSMM</td>
<td>32.27%</td>
<td>95.3%</td>
<td>48.21%</td>
<td>$4.63 \times 10^{-4}$</td>
</tr>
<tr>
<td>M2</td>
<td>PreFix</td>
<td>59.79%</td>
<td>58.59%</td>
<td>59.18%</td>
<td>$5.43 \times 10^{-6}$</td>
</tr>
<tr>
<td></td>
<td>SKSVM</td>
<td>4.47%</td>
<td>8.72%</td>
<td>5.91%</td>
<td>$2.57 \times 10^{-5}$</td>
</tr>
<tr>
<td></td>
<td>HSMM</td>
<td>0.28%</td>
<td>60.58%</td>
<td>0.56%</td>
<td>$2.94 \times 10^{-3}$</td>
</tr>
<tr>
<td>M3</td>
<td>PreFix</td>
<td>84.00%</td>
<td>52.50%</td>
<td>64.61%</td>
<td>$2.48 \times 10^{-5}$</td>
</tr>
<tr>
<td></td>
<td>SKSVM</td>
<td>0.79%</td>
<td>91.91%</td>
<td>1.58%</td>
<td>$2.85 \times 10^{-2}$</td>
</tr>
<tr>
<td></td>
<td>HSMM</td>
<td>26.32%</td>
<td>11.11%</td>
<td>15.63%</td>
<td>$7.72 \times 10^{-5}$</td>
</tr>
</tbody>
</table>
Evaluation Experiments

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Method</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Pre-Fix</td>
<td>87.35%</td>
<td>74.26%</td>
<td>80.23%</td>
<td>8.42 x 10^{-5}</td>
</tr>
<tr>
<td>M3</td>
<td>SVM</td>
<td>97.79%</td>
<td>91.91%</td>
<td>1.58%</td>
<td>2.83 x 10^{-5}</td>
</tr>
<tr>
<td>HSMM</td>
<td></td>
<td>26.32%</td>
<td>11.11%</td>
<td>15.63%</td>
<td>7.72 x 10^{-5}</td>
</tr>
</tbody>
</table>

Average recall: 61.81%, mean time between false alarms (for a single switch): 8494 days (23.3 years)
Conclusion

Challenges

• Noisy signals in syslog data
• Sample imbalance

Four features

• Sequence, seasonality, surge and frequency
• LCS² method

Evaluation

• Real-world data

Future work

• Switch failure prediction across different switch models
Thank you!

Q&A

zhangsl@nankai.edu.cn
Backups
Focus on switch hardware failures

External problems
• Power supply down

Configuration problems
• VPN tunneling errors

Hardware failures
• Crash induced by hardware errors
  • Line card crash
  • Entire switch crash

Software crash
• Due to bugs

Generated by operators and other devices

Automatically recover (via a reboot)
To the best of our knowledge, in the literature there are no previous works on failure prediction within switch models. Consequently, to demonstrate the performance of PreFix, we compare PreFix with benchmark methods for switches in data center networks. That is, we do not have benchmark methods for each switch model, we collect the data from switches across almost infeasible to compare the performance of PreFix among different data centers. As a result, for a specific data center, the failure cases are too few to train a failure prediction model. Therefore, it is important to ensure that our experiments are reproducible, we have built a website which contains all the data applied in the evaluation, including the historical switch failures, message templates and message template sequences of all the three switch models. Please note that for a specific data center, the failure cases are too few to train a failure prediction model. Consequently, we set a setting as follows. Based on empirical experience, we simulate the online prediction procedure, in the evaluation experiments we slide a time bin which contains no less than 5 syslog messages. On the one hand, if the number of omen time bins is too small, e.g., about 50% of switch failures do not have any omen time bin, the number of omen time bins will be divided by the length of each time bin to capture the omen pattern, and thus cannot be used for failure prediction. On the other hand, if the number of omen time bins is too large, e.g., all data centers have no omen time bin, there will be too few time bins with more than 5 syslog messages in a time bin's corresponding message sequence, the message sequence would be too intensive. The operators need at most 30 minutes to react to a positive failure prediction, such as shifting the monitoring syslogs of a 24 hours' period for the online prediction procedure is not always available. The operators believe that syslogs within 24 hours before a given failure can capture the omen pattern. In addition, we find that, in most cases (more than 90%), syslogs in any two hours among the dozens of failures, we found that, in most cases (more than 90%), syslogs in any two hours among the dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours before a failure are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours before a failure are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours before a failure are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours before a failure are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours before a failure are indicative of the failures, and thus can be used for failure prediction. After analyzing the syslogs before dozens of failures, we found that, in most cases (more than 90%), syslogs within 24 hours before a failure are indicative of the failures, and thus can be used for failure prediction.

### Detailed information for the three models of switches

<table>
<thead>
<tr>
<th>Switch model</th>
<th># failures</th>
<th># failed switches</th>
<th># switches in total</th>
<th># Omen time bins</th>
<th># Non-omen time bins</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>228</td>
<td>131</td>
<td>2223</td>
<td>1273</td>
<td>5,516,435</td>
</tr>
<tr>
<td>M2</td>
<td>48</td>
<td>30</td>
<td>3288</td>
<td>317</td>
<td>22,997,509</td>
</tr>
<tr>
<td>M3</td>
<td>139</td>
<td>31</td>
<td>3886</td>
<td>164</td>
<td>660,736</td>
</tr>
</tbody>
</table>
Comparison of the Importance of the Four Features

Table 10. Normalized node impurity decrease of the features in the RF model

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Sequence</th>
<th>Frequency&amp;Seasonality</th>
<th>Surge&amp;Seasonality</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>22.29%</td>
<td>51.14%</td>
<td>26.57%</td>
</tr>
<tr>
<td>M2</td>
<td>19.09%</td>
<td>50.25%</td>
<td>30.65%</td>
</tr>
<tr>
<td>M3</td>
<td>42.81%</td>
<td>36.86%</td>
<td>20.33%</td>
</tr>
</tbody>
</table>
Fig. 2. The model of switch failure prediction. For a given switch failure that occurred at \(\tau_h\), our objective is to predict the failure during \([\tau_s, \tau_e]\). \(\tau_e\) is \(\Delta \tau_a\) before \(\tau_h\) because network operators need no more than \(\Delta \tau_a\) time to react to a positive failure prediction. In the offline learning procedure, given the failure at \(\tau_h\), for any \(\tau_x\) in \([\tau_s, \tau_e]\), the syslog message sequence in \([\tau_x - \Delta \tau_m, \tau_x]\) is labeled as an omen message sequence, while the syslog message sequence in \([\tau_y - \Delta \tau_m, \tau_y]\) is labeled as a non-omen message sequence when \(\tau_y \notin [\tau_s, \tau_h]\).