Model-based anomaly detection in response delay in communication through LTE network

Kohei Yamamoto*, Naoki Wakamiya†
Graduate School of Information Science and Technology,
Osaka University
1-5 Yamadaoka, Suita-shi, Osaka 565-0871, Japan
{*k-yamamt, †wakamiya}@ist.osaka-u.ac.jp

Ryo Nakano‡, Ryosuke Fujiwara§
Research & Development Group, Hitachi, Ltd.
1-280 Higashikoigakubo, Kokubunji-shi, Tokyo 185-8601, Japan
{‡ryo.nakano.xd, §ryosuke.fujiwara.mb}@hitachi.com

***Abstract*—Industrial monitoring systems are developed and deployed to continuously and remotely monitor the status of industrial equipment and detect failures. A gateway node collects status data from sensors attached to machines and then sends them to a server for analysis and evaluation. In this paper, we propose a method to detect anomalies in communication between a gateway and a server over an LTE network, whose failure would bring a serious result such as an operation halt of the whole factory. We model a time series of dynamically and instantaneously changing response delay as sawtooth waves and detect an anomaly based on their statistical characteristics. Through evaluations using real measurements and artificial data, we verified that our method can detect both of constant increase and decrease, rapid increase, long-term increase, and slow decrease in the response delay.**

***Index Terms*—industrial monitering system, Long Term Evolution, response delay, model-based anomaly detection**

I. Introduction

Recently industrial monitoring systems [1] are widely deployed for fast detection of abnormal condition such as a failure of a machine and reduction of personnel cost in inspection. However, a communication failure such as extraordinary delay and disconnection would bring a serious and irretrievable result causing a halt of the factory. In this paper, we focus on anomaly detection in communication from a gateway placed at a factory to a cloud server through an LTE (Long Term Evolution) network, which is widely used as the backhaul. There have been several attempts to analyze the characteristics of an LTE network and detect anomalies. For example, in [2], they analyzed a mechanism of instantaneous increase in the delay and proposed a method to reduce its occurrence by controlling packet size and transmission interval based on radio quality. In [3], they proposed a machine learning based method to predict a drop of a session between a user equipment and a base station.

In this paper, we first propose a method to model a time series of dynamically changing response delay measured in communication between a gateway and a cloud server through an LTE network. More specifically we focus on a specific characteristic of a time series of response delay to form sawtooth-like waves, that is, a gradual increase followed by quick decrease of delay. We model a time series of instantaneous response delay measurements by a time series of sawtooth waves, which is expressed by a set of characteristic values, that is, a starting point delay, a slope gradient, a slope width, a gap width, and an end point delay. Next we propose an anomaly detection method to identify irregular delay based on statistical properties of sawtooth waves. For this purpose, we define the anomaly score using the Mahalanobis distance and adopt a threshold-based detection algorithm.

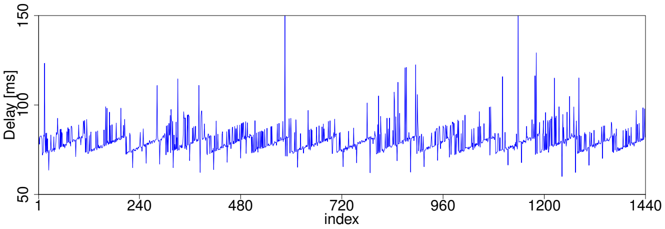


Fig. 1. Measured response delay (from 0 am to 6 am, Tuesday 23rd June)

The paper is organized as follows. First section II introduces a feature extraction method to extract sawtooth waves from a time series of response delay. Next in section III we propose an anomaly detection method and verify its performance using real and artificial data. Finally section IV summarizes the paper and shows future direction.

II. Feature extraction from response delay data

First, we conducted measurements in the environment similar to an industrial monitoring system. We used a Raspberry Pi equipped with Quectel's EC21-J LTE module as a wireless device for a gateway and an AWS server as a cloud server. The Raspberry Pi was placed in our laboratory at Osaka University. Every 15 seconds the Raspberry Pi first obtains a timestamp and then executes a Ping command (packet size 60 bytes including the header, ICMP_ECHO, one packet) to measure the response delay of a connection to the AWS server via an LTE network of IIJ Mobile's Service Type D [4].

The measurements lasted for four weeks from Tuesday 23rd June to Wednesday 22nd July 2020. In total, we obtained 172,800 measurements. However, because some measurements failed due to malfunctions of the Raspberry Pi, we used valid 167,427 measurements. An example of a time series of obtained response delay is illustrated in Fig. 1.

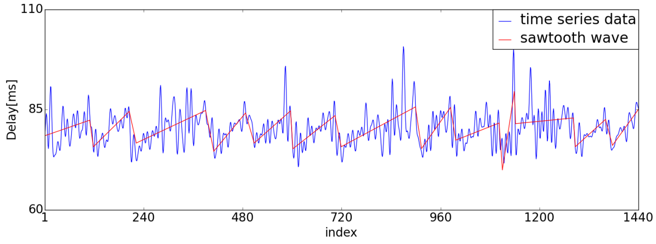


Fig. 2. Extracted sawtooth wave

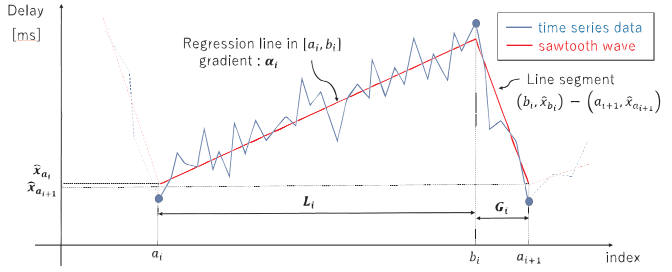

Delay [ms]
Regression line in $[a_i, b_i]$ gradient : α_i
Line segment $(b_i, \hat{x}_{b_i}) - (a_{i+1}, \hat{x}_{a_{i+1}})$
time series data
sawtooth wave
$\hat{x}_{a_i}$
$\hat{x}_{a_{i+1}}$
L_i
G_i
a_i
b_i
a_{i+1}
index

Fig. 3. Characteristic values of ith sawtooth wave

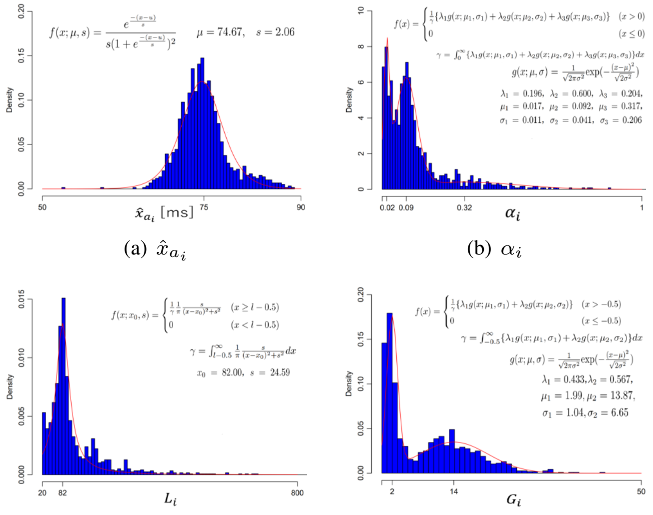
A. Sawtooth wave extraction algorithm

In extracting sawtooth waves, first to eliminate instantaneous fluctuations a low-pass filter is applied to a time series of measured response delay. In this paper we use 0.008 Hz as the cutoff frequency based on the power spectrum and the smoothness of the obtained results. As an example, a result of application of the low-pass filter to Fig. 1 is shown in Fig. 2. Hereafter we write a time series of response delay after applying the low-pass filter as $\{x_1, x_2, \ldots, x_n\}$, where n is the number of measured values.

Next sawtooth waves are extracted from the time series. The ith sawtooth wave is represented by five values as shown in Fig. 3. They are the starting point delay $\hat{x}_{a_i}$ whose position is a_i, the slope gradient α_i, the slope width L_i from the starting point position a_i to the position b_i of the peak in delay, the gap width G_i from the peak position b_i to the starting point position a_{i+1} of the next sawtooth wave, and the end point delay $\hat{x}_{a_{i+1}}$ at a_{i+1}.

The starting point a_i is determined based on gradients of regression lines. When the range of regression $[k, k+l]$ is moved from $k = b_{i-1}$, a peak of the preceding sawtooth wave, one by one, the gradient of a regression line first increases from a negative value, next changes to a positive value, and then becomes stable on reaching the next slope. l is a constant and set at the typical sawtooth width. A point where the gradient becomes stable is considered a_i. Because of the space limitation, the detailed algorithm is not shown in the paper.

The peak position b_i is determined based on gradients of regression lines as well. Fixing the left end of regression at the starting point a_i and expanding the range of regression one by one, the gradient of a regression line continuously decreases after the right end of the regression range exceeds the peak. Then, the slope width L_i is derived as $b_i - a_i + 1$.



(a) $\hat{x}_{a_i}$

(b) α_i

(c) L_i

(d) G_i

Fig. 4. Probability distribution of characteristic values

The regression line $\hat{x}_j = \alpha_i j + c_i$ is obtained in the range $[a_i, b_i]$, where α_i means the slope gradient of the ith sawtooth wave. It must be noted that the starting point delay of the ith sawtooth wave is not x_{a_i} in analysis but $\hat{x}_{a_i}$ obtained by substituting the starting point a_i to the regression line function. Finally, the starting point position a_{i+1} of the next sawtooth wave is determined and the gap width G_i is derived as $a_{i+1} - b_i - 1$. Figure 2 shows an example of extracted sawtooth waves by red zigzag lines.

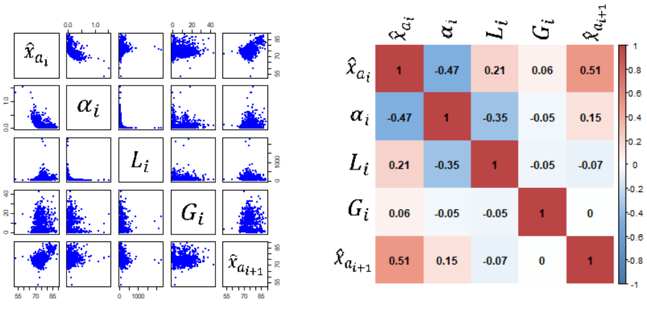
B. Statistical characteristics of sawtooth waves

The probability distributions of characteristic values of extracted sawtooth waves are summarized in Fig. 4. Red lines show probability density functions obtained by fitting, whose exact functions are shown in the figure to save space. As shown in the figure, the starting point delay follows the logistic distribution, the slope gradient and the gap width follow the mixture Gaussian distribution, and the slope width follows the Cauchy distribution.

A scatter plot and a correlation matrix are shown in Fig. 5. As shown, there is positive correlation between the starting point delays $\hat{x}_{a_i}$ and $\hat{x}_{a_{i+1}}$. It means that there is a midterm trend in response delay and it is not fully random. In addition, there exist negative correlations between the staring point delay $\hat{x}_{a_i}$ and the slope gradient α_i and between the slope gradient α_i and the slope width L_i, respectively. It is because there is a kind of upper limit in the response delay in usual conditions. Therefore, when the starting point delay is large, the slope gradient becomes small, for example.

III. Anomaly Detection in Response Delay

In this section we propose an anomaly detection method which uses statistical properties of sawtooth waves extracted from measured response delay.



(a) scatter plot

(b) correlation coefficient

Fig. 5. Correlation between characteristic values

A. Anomaly detection method

An anomaly score of a sawtooth wave extracted from a time series of measured response delay is determined base on its statistical distance to training data obtained in the usual condition. As a distance measure of multivariate analysis we use the Mahalanobis distance [5].

To obtain reference data, characteristic values of sawtooth waves of training data are first normalized to have the distribution with mean 0 and variance 1 by the Z-score normalization. We divide sawtooth waves into six groups, because there are three and two peaks in the distributions of the slope gradient α_i and the gap width G_i, respectively.

In anomaly detection, a time series of response delay is first obtained by realtime measurement. Next, a sawtooth wave is extracted by the feature extraction method explained in section II. Then, the anomaly score of the sawtooth wave is derived as the minimum of the Mahalanobis distances from normalized characteristic values of the wave to the six groups. Finally, an anomaly is considered to happen when the anomaly score exceeds the predetermined threshold.

B. Detection results

We used measurements obtained from Tuesday 23rd June to Wednesday 15th July as training data. Then we applied our anomaly detection method to the training data, the test data which are obtained from Thursday 16th July to Wednesday 22nd July, and the artificial data generated following the statistical characteristics shown in II-B. Since it is not possible to intentionally cause failures of the LTE network under operation, we changed statistical characteristics of the artificial data to imitate unusual conditions of communication through an LTE network. In evaluation we used the percentage of anomalies, that is, sawtooth waves whose anomaly score exceeds the threshold. The threshold was tentatively set at 5 based on preliminary evaluation.

1) anomaly scores of training data, test data, and artificial data: Figure 6 shows an example of a time series of x_i (blue line), extracted sawtooth waves (red line), and the corresponding anomaly scores (black line). In this case all sawtooth waves are considered normal for their anomaly scores lower than 5. In Fig. 7(a), a box plot of anomaly scores of the training data is shown. Our method considers the most of training data as normal as we expected. About 0.5% of sawtooth waves have the anomaly score larger than 5, but it is mainly because of extraction failures. Regarding test data, the percentage of anomalies is about 0.9% as shown in Fig. 7(b). Therefore, the test data is also regarded as normal. The percentage of anomalies of artificial data is about 1.1% as shown in Fig. 7(c), meaning that the artificial data have the similar characteristics with real measurements.

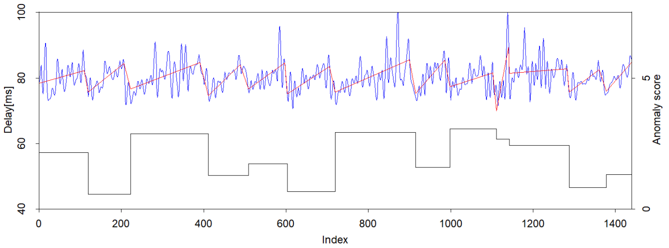
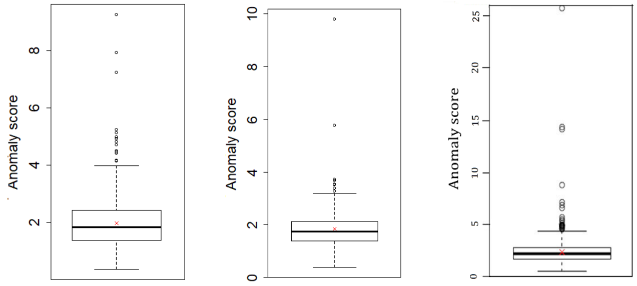


Fig. 6. Transition of the anomaly score (training data)



(a) training data (n = 903)

(b) test data ($n = 233$)

(c) artificial data (n = 1000)

Fig. 7. Box plot of the anomaly score

2) anomaly scores of artificial anomalies: To verify that our method can detect anomalies, we changed statistical characteristics of artificial data based on scenarios S1 to S10. Results are summarized in Tables I to III.

S1: $\hat{x}_{a_i} \times A, \alpha_i \times A, L_i \times A$, or $G_i \times A$, $0.5 \leq A \leq 2$.
S2: $\hat{x}_{a_i} + A$, $-30 \leq A \leq 60$ ms.
S3: $\hat{x}_{a_i} + A$ and $\alpha_i \times B$, $-30 \leq A \leq 60$ ms, $0.5 \leq B \leq 2$.
S4: $\alpha_i \times A$ and $L_i \times A$, $0.5 \leq A \leq 2$.
S5: Var($\hat{x}_{a_i}$) $\times A$, Var(α_i) $\times A$, Var(L_i) $\times A$, or Var(G_i) $\times A$, $0.5 \leq A \leq 2$.
S6: change normalized Cor($\hat{x}_{a_i}, \hat{x}_{a_{i+1}}$) from -1 to 1.
S7: change normalized Cor($\hat{x}_{a_i}, \alpha_i$) from -1 to 1.
S8: change normalized Cor(α_i, L_i) from -1 to 1.
S9: Var(η_i) $\times A$, $0.5 \leq A \leq 2$. η_i is a random variable added to artificial sawtooth waves and follows the normal distribution with mean -0.03 and variance of 4.2.
S10: Add a spike-shaped delay with probability p, $0.1\% \leq p \leq 5\%$.

Regarding S1 through S4, our method is sensitive to changes

TABLE I
ANOMALY[%] OF SCENARIOS FROM S1 TO S5

multiple and/or addition [ms]	0.5 -30	0.75 -15	1 0	1.25 15	1.5 30	1.75 45	2 60
S1 $\hat{x}_{a_i}$	100	85.9	1.1	7.1	100	100	100
S1 α_i	1.1	1.2	1.1	2.1	2.7	4.5	7.5
S1 L_i	0.4	0.7	1.1	2.5	4.7	8.7	15
S1 G_i	1.2	1	1.1	1.5	2.4	4.6	9.1
S2	100	43.5	1.1	35.8	99.9	100	100
S3	100	48.3	1.1	44.3	100	100	100
S4	0.6	0.7	1.1	4	12.7	33.9	60.4
S5 $\hat{x}_{a_i}$	4	3.9	1.1	3.8	2.3	4.3	4.2
S5 α_i	2.3	3.3	1.1	4.9	6.7	7.1	8.2
S5 L_i	3.5	3.9	1.1	4.5	4.3	5.7	6.1
S5 G_i	2.7	3.4	1.1	3.1	3.9	3.6	5

TABLE II
ANOMALY[%] OF SCENARIOS S6, S7, AND S8

corr. coef. converted to $N(0,1)$		-1	-0.75	-0.5	0.5	0.75	1
S6	corr. coef.	-1	-0.77	-0.49	0.53	0.71	0.98
	anomaly[%]	0.6	7.1	4.8	1.1	1.1	1.4
S7	corr. coef.	-0.86	-0.62	-0.39	0.42	0.63	0.88
	anomaly[%]	1	1.3	1.1	2.7	5.2	3.5
S8	corr. coef.	-0.09	-0.21	-0.04	0.23	0.32	0.48
	anomaly[%]	1.2	1.1	4.8	13.3	14.4	19.3

TABLE III
ANOMALY[%] OF SCENARIOS OF S9 AND S10

multiple	0.5	1	1.5	-	-	base
S9	2.6	6	16	-	-	1

rate[%]	0.1	0.5	1	3	5	base
S10	9.9	8.4	9.9	12.7	14.1	1.8

in the response delay (S1 $\hat{x}_{a_i}$, S2, and S3) where the percentage of anomalies significantly increases by the manipulations as shown in Table I. It is because those manipulations change the distribution of $\hat{x}_{a_i}$ enough to make the difference to the original distribution very large. On the contrary, the percentage of anomalies does not change much or even decreases with small multipliers in S1 on α_i, L_i, and G_i and S4. It is because the modified distribution overlaps with the original and thus the statistical difference is small. With large multipliers the percentage of anomalies increases in those scenarios. It means that the rapid or long-term increases in the response delay as well as the slow decrease are likely to be detected as unusual, which is more harmful than the opposite situation, that is, the slow or short-term increase and the fast decrease in the response delay. In the case of S4, the degree of increase in the percentage of anomalies is higher than those in S1 on α_i and L_i, because the manipulation changes the multivariate distribution of them.

On the other hand, based on results of S5, the influence of a change in distribution on the percentage of anomalies is not as significant as in S1. Since the mean of the modified distribution is kept at the same position as the original distribution in the variance manipulation, the statistical difference is small the anomaly score does not increase very much.

In Table II, the sensitivity of the anomaly detection method to a change in correlation is not high except for the case of increasing the correlation in S8. It is mainly because of the wide distribution of characteristic values as shown in the scatter plot of Fig. 5. Changing the correlation does not cause significant difference in their relative distributions. Consequently, the percentage of anomalies does not change much. In the case of S8, because of the narrow bivariate distribution of the slope angle α_i and the slope width L_i, especially increasing the correlation results in the increase in the percentage of anomalies.

As shown in Table III, increasing the variance of the noise and the occurrence rate of instantaneous increasing response delay made the percentage of anomalies slightly high. The main reason of the small change is that our feature extraction method often fails in extracting sawtooth waves. Because of the increased variance and additional spikes, the gradient of a regression line becomes less stable. Such extraction failures can be regarded as a sign of anomaly.

IV. CONCLUSION AND FUTURE WORK

In this paper, we proposed the anomaly detection method which uses statistical characteristics of sawtooth waves extracted from a time series of response delay measurements. We showed that our method can detect both increase and decrease in the response delay very well when the degree of change is more than about 20%. Furthermore, it can detect rapid increase, long-term increase, and slow decrease in the response delay as a trend different from the usual condition. On the other hand, it was not possible to detect irregular fluctuations in the instantaneous response delay.

As future work we plan to evaluate our proposal in other environments, for example, with poor wireless signal. We will investigate how a time series of response delay and statistical characteristics of extracted sawtooth waves change depending on the environmental condition. In addition, we also need to improve the feature extraction method.

REFERENCES

[1] A.C. Lima-Filho, R.D. Gomes, M.O. Adissi, T.A. da Silva, F.A. Belo, and M.A. Spohn, “Embedded system integrated into a wireless sensor network for online dynamic torque and efficiency monitoring in induction motors,” *IEEE/ASME Transactions on Mechatronics*, vol. 17, no. 3, pp. 404–414, Apr 2012.

[2] N. Koichi and S. Kozo, “Study on mechanism and reduction approaches of delay spikes occurrence on mobile networks,” *in Proceedings of the 13th International Conference on Telecommunications, ConTEL 2015*, pp. 1–7, July 2015.

[3] D. Balint, V. Peter, and B. Andras, “Machine learning based session drop prediction in LTE networks and its SON aspects,” *IEEE Vehicular Technology Conference*, vol. 2015, pp. 3–7, May 2015.

[4] Internet Initiative Japan Inc., “IIJ mobile service type D / type K,” https://www.iij.ad.jp/en/biz/iijmobile-dk/.

[5] R. de Maesschalck, D. Jouan-Rimbaud, and D.L. Massart, “The mahalanobis distance,” *Chemometrics and intelligent laboratory systems*, vol. 50, no. 1, pp. 1–18, 2000.