Deep Learning Based Anomaly Detection Technology for ICT Services—DeAnoS: Deep Anomaly Surveillance

Keishiro Watanabe, Kengo Tajiri, and Yuusuke Nakano

Abstract

In this article, we outline a deep learning based anomaly detection technology called Deep Anomaly Surveillance (DeAnoS). The NTT laboratories have been developing this technology with the aim of enabling proactive maintenance operations for ICT (information and communication technology) services. The present situation regarding verification of DeAnoS at NTT Group companies is also explained.

Keywords: Network-AI, network and service operations, anomaly detection

1. Introduction

NTT Network Technology Laboratories is developing a deep learning based anomaly detection technology called Deep Anomaly Surveillance (DeAnoS), which utilizes an autoencoder (AE) to promptly detect changes in the state of an ICT (information and communication technology) service [1–3]. In this article, we explain the technical issues concerning DeAnoS, which was exhibited at NTT R&D Forum 2018 Autumn held in November 2018.

2. Overview of DeAnoS

An AE, as used in DeAnoS, is a type of deep learning based neural network that enables the learning of complicated structures inherent in data. Attention is now being focused on the use of AEs in technology for detecting anomalies. When an AE is used, the dimensionality of data in the middle layer of the AE is reduced by setting the dimensionality of the middle layer to be less than that of the input and output layers and by learning the parameters for reproducing the data of the input layer in the output layer. Anomaly detection using an AE is based on the premise that normal data are distributed in the input-data space around certain manifolds that can express low dimensions. Specifically, as shown in **Fig. 1**, at the time of learning, a *normal* state is learned by using various kinds of data observed during normal operation of the system, and at the time of the test (i.e., anomaly detection), the current data are input to the AE that has learned the normal state as described above, and the distance between vectors of the input and output layers is output as the anomaly degree. When the degree of anomaly exceeds the threshold, the state is detected as an anomaly.

In addition to numerical data such as resource and traffic information based on SNMP (Simple Network Management Protocol)/MIB (Management Information Base) and flow data based on Netflow, the network data to be entered also include the syslog of routers and servers (text information). With text logs such as syslog, identifiers (IDs) are created by using syslog-analysis technology [4] for each syslog line, and the text log is converted to numerical data by using the appearance frequency of each ID. This process enables learning of information including syslog.

We are also working on not only detecting anomalies

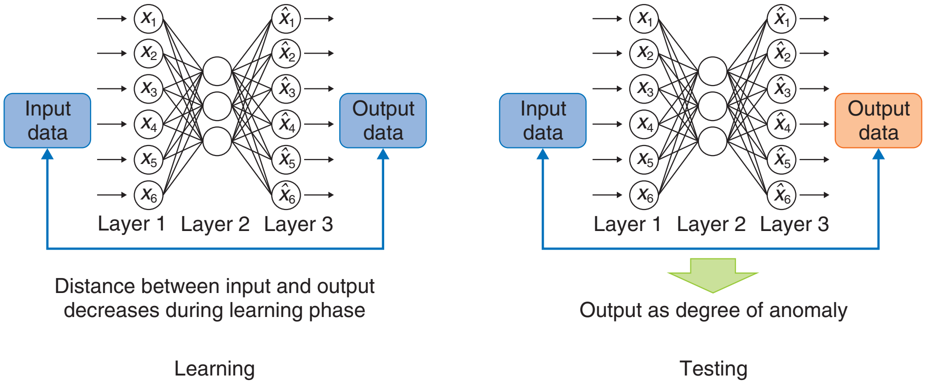
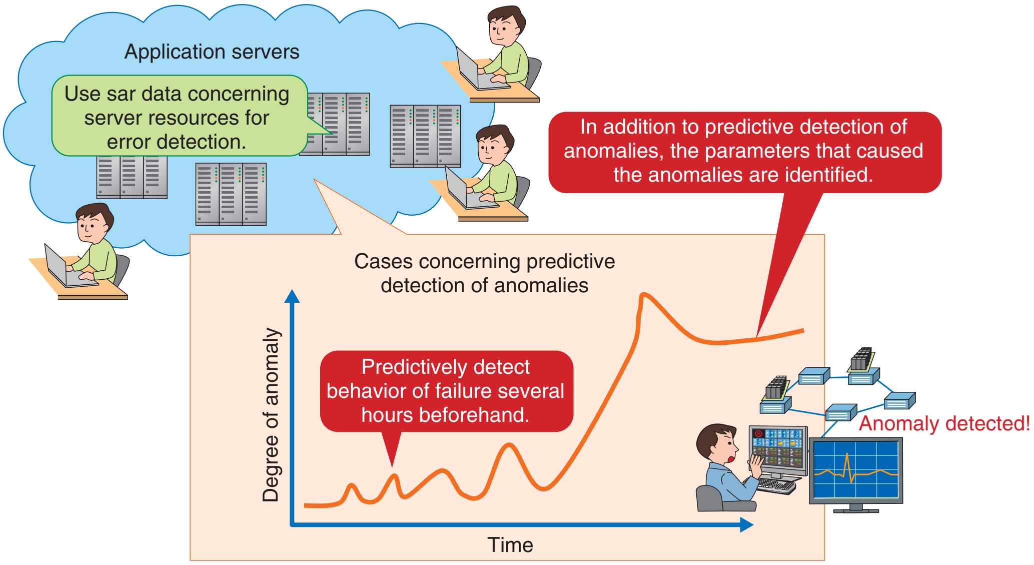

Input data
Output data
x_1 x_2 x_3 x_4 x_5 x_6
$\hat{x}_1$ $\hat{x}_2$ $\hat{x}_3$ $\hat{x}_4$ $\hat{x}_5$ $\hat{x}_6$
Layer 1 Layer 2 Layer 3
Distance between input and output decreases during learning phase
Learning
Output as degree of anomaly
Testing

Fig. 1. How an AE works.


Application servers
Use sar data concerning server resources for error detection.
In addition to predictive detection of anomalies, the parameters that caused the anomalies are identified.
Cases concerning predictive detection of anomalies
Degree of anomaly
Predictively detect behavior of failure several hours beforehand.
Anomaly detected!
Time

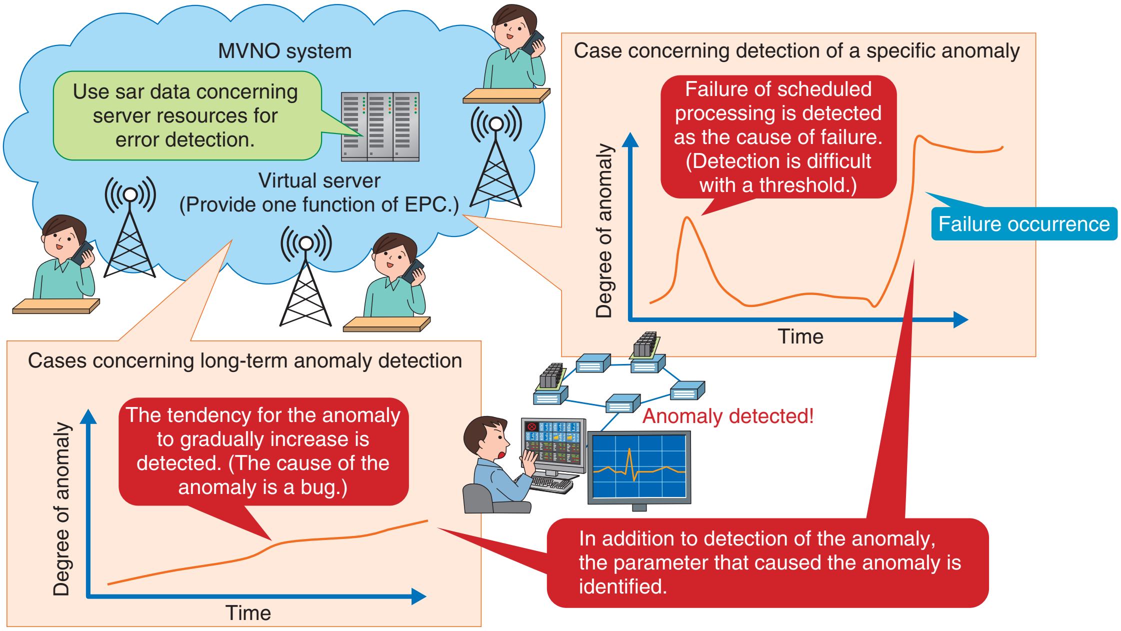
sar: system admin reporter

Fig. 2. Initiative with Strategic Network Management Department of NTT EAST.

but also estimating their cause at the time they are detected [5, 6]. Specifically, we are investigating a method using sparse optimization for estimating which input dimension causes the anomaly degree to become higher when an anomaly is detected by the AE. With this technology, the degree of contribution of each input dimension to the degree of anomaly is calculated; accordingly, it is expected to improve the efficiency of investigation after detection of anomalies.

3. Status of verification of DeAnoS at NTT Group companies

In cooperation with NTT Group companies, we are presently verifying DeAnoS on the basis of operational data acquired from actual services, and we are assessing the effectiveness of this technology and extracting the issues for practical use. Our initiatives with the Strategic Network Management Department of NTT EAST and the Network Services Department of NTT Communications are shown in **Figs. 2** and **3**, respectively. First, in cooperation with the Strategic


MVNO system
Use sar data concerning server resources for error detection.
Virtual server (Provide one function of EPC.)
Case concerning detection of a specific anomaly
Failure of scheduled processing is detected as the cause of failure. (Detection is difficult with a threshold.)
Failure occurrence
Degree of anomaly
Time
Cases concerning long-term anomaly detection
The tendency for the anomaly to gradually increase is detected. (The cause of the anomaly is a bug.)
Degree of anomaly
Time
Anomaly detected!
In addition to detection of the anomaly, the parameter that caused the anomaly is identified.

EPC: evolved packet core
MVNO: mobile virtual network operator

Fig. 3. Initiative with Network Services Department of NTT Communications.

Network Management Department of NTT EAST, we confirmed the effectiveness of DeAnoS in detecting anomalies in application servers and estimating the parameters that caused them. Second, in an initiative with the Network Services Department of NTT Communications, we confirmed a case in which it was possible to estimate the causal parameter in addition to detecting the anomaly by analyzing changes in specific events and long-term trends.

4. Future prospects

In this article, the deep learning based technology DeAnoS, which NTT Network Technology Laboratories has been developing, was outlined, and the situation regarding its verification at NTT Group companies concerning network-anomaly detection technology was described. We will continue to fine tune DeAnoS by proceeding with its technology verification with the aforementioned companies and improve the environment for utilizing DeAnoS in the real world. Future tasks regarding technology for detecting network anomalies are to (i) improve the interpretability of main causes when an anomaly is detected and (ii) adapt such technology to various environments. Accordingly, we will continue our research and development to address those issues.

References

[1] Y. Nakano, Y. Ikeda, K. Watanabe, K. Ishibashi, and R. Kawahara, “Autoencoder Based Detection Method for Network Anomalies,” Proc. of the 2017 IEICE General Conference, B-7-33, Nagoya, Aichi, Japan, Mar. 2017 (in Japanese).

[2] Y. Ikeda, Y. Nakano, K. Watanabe, K. Ishibashi, and R. Kawahara, “A Study of Accuracy Improvement on Network Anomaly Detection with Autoencoder,” Proc. of the 2017 IEICE General Conference, B-7-34, Nagoya, Aichi, Japan, Mar. 2017 (in Japanese).

[3] R. Kawahara, “Application of AI/Machine Learning to Enhance Network Operation/Control Technologies,” Proc. of the 2017 IEICE Society Conference, BT-2-1, Tokyo, Japan, Sept. 2017 (in Japanese).

[4] T. Kimura, A. Watanabe, T. Toyono, and K. Ishibashi, “Proactive Failure Detection Learning Generation Patterns of Large-scale Network Logs,” Proc. of the 11th International Conference on Network and Service Management (CNSM 2015), Barcelona, Spain, Nov. 2015.

[5] Y. Ikeda, K. Ishibashi, Y. Nakano, K. Watanabe, and R. Kawahara, “Inferring Causal Parameters of Anomalies Detected by Autoencoder Using Sparse Optimization,” IEICE Technical Report, Vol. 117, No. 89, pp. 61–66, 2017 (in Japanese).

[6] Y. Ikeda, K. Ishibashi, Y. Nakano, K. Watanabe, and R. Kawahara, “Anomaly Detection and Interpretation Using Multimodal Autoencoder and Sparse Optimization,” arXiv:1812.07136 [stat.ML], 2018.

Keishiro Watanabe

Senior Research Engineer, NTT Network Technology Laboratories.

He received a B.E. and M.E. in satellite communications from Kyushu University, Fukuoka, in 2002 and 2004. After joining NTT in 2004, he conducted research on network management and quality of experience. He was with NTT Communications from 2012 to 2015. He is now working on the development of sophisticated operations of network systems by using artificial intelligence. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Kengo Tajiri

NTT Network Technology Laboratories.

He received an M.E. in physics from Kyoto University in 2017. Since joining NTT in 2017, he has been engaged in research on traffic analysis for telecommunication networks. He is a member of IEICE.

Yuusuke Nakano

Research Engineer, NTT Network Technology Laboratories.

He received an M.E. in system engineering from Wakayama University in 2005 and a Ph.D. in information science and technology from Osaka University in 2011. He joined NTT Network Service Systems Laboratories in 2005. His research interests include network anomaly detection and web performance measurement and acceleration. He is a member of IEICE and the Information Processing Society of Japan.