(12) STANDARD PATENT (11) Application No. **AU 2021432832 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
ESTIMATION APPARATUS, ESTIMATION METHOD, AND PROGRAM

(51) International Patent Classification(s)
H04L 1/00 (2006.01)

(21) Application No: **2021432832** (22) Date of Filing: **2021.03.09**

(87) WIPO No: **WO22/190198**

(43) Publication Date: **2022.09.15**
(44) Accepted Journal Date: **2024.09.26**

(71) Applicant(s)
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

(72) Inventor(s)
YAMANAKA Yuki

(74) Agent / Attorney
Spruson & Ferguson, GPO Box 3898, Sydney, NSW, 2001, AU

(56) Related Art
US 20190044913 A1
JP 2019110513 A
US 2021/0203605 A1
US 2014/0082730 A1

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年9月15日(15.09.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/190198 A1

(51) 国際特許分類:
H04L 12/70 (2013.01)

(21) 国際出願番号： PCT/JP2021/009228

(22) 国際出願日： 2021年3月9日(09.03.2021)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

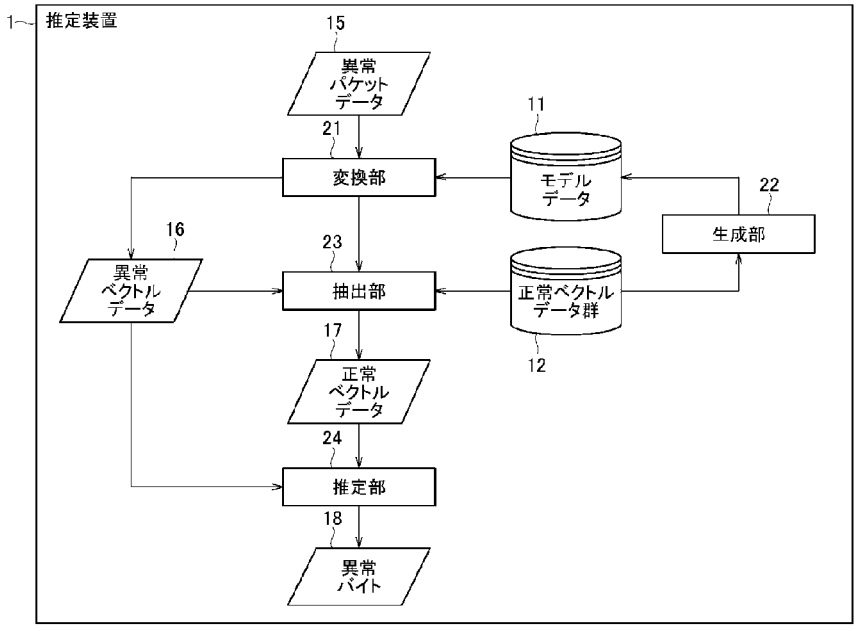
(72) 発明者: 山中 友貴 (**YAMANAKA Yuki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

(74) 代理人: 三好 秀和，外 (**MIYOSHI Hidekazu** et al.); 〒1050001 東京都港区虎ノ門１丁目２番８号 虎ノ門琴平タワー Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) **Title:** ESTIMATION DEVICE, ESTIMATION METHOD AND PROGRAM

(54) 発明の名称： 推定装置、推定方法およびプログラム



1 Estimation device
11 Model data
12 Normal vector data group
15 Abnormal packet data
16 Abnormal vector data
17 Normal vector data
18 Abnormal byte
21 Conversion unit
22 Generation unit
23 Extraction unit
24 Estimation unit

(57) **Abstract:** An estimation device 1 comprises: a conversion unit 21 that converts abnormal packet data 15 into abnormal vector data 16 by using a model for converting packet data into vector data in which a vector representing a feature of the value of each byte of the packet data is associated with the byte; an extraction unit 23 that extracts, from a plurality of pieces of normal vector data into which a plurality of pieces of normal packet data have been converted by using the model, normal vector data 17 having a relatively high similarity to the abnormal vector data 16; and an estimation unit

WO 2022/190198 A1

［続葉有］

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

24 that estimates an abnormal byte in the abnormal packet data 15 from the similarity between a vector corresponding to each byte of the abnormal vector data 16 and a vector corresponding to each byte of the extracted normal vector data 17.

(57) 要約:推定装置１は、パケットデータを、前記パケットデータの各バイトに、各バイトの値の特徴を表す各ベクトルを対応づけるベクトルデータに変換するモデルを用いて、異常パケットデータ１５を異常ベクトルデータ１６変換する変換部２１と、複数の正常パケットデータが前記モデルを用いて変換された複数の正常ベクトルデータから、異常ベクトルデータ１６の類似度が相対的に高い正常ベクトルデータ１７抽出する抽出部２３、異常ベクトルデータ１６の各バイトに対応するベクトルと、抽出された正常ベクトルデータ１７の各バイトに対応するベクトルとの類似度から、異常パケットデータ１５における異常バイトを推定する推定部２４を備える。

Description

Title of Invention

ESTIMATION APPARATUS, ESTIMATION METHOD, AND PROGRAM

Technical Field

[0001]

The present invention relates to an estimation apparatus, an estimation method, and a program.

Background Art

[0002]

In a communication network of an operational technology (OT) in an industrial system, a building system, or the like, an abnormality detection system or an intrusion detection system (operational technology intrusion detection system (OT-IDS)) has attracted attention. Packets transmitted and received in such a communication network need to be detected without overlooking even a small amount of unauthorized rewriting such as one byte. For example, an unexpected operation may cause a serious accident, such as a case where a set value of temperature is changed by one digit due to unauthorized rewriting.

[0003]

There are tools for monitoring a network (refer to Non Patent Literature 1 and Non Patent Literature 2).

2021432832 04 Sep 2024

These tools can monitor and analyze data transmitted and received via the network.

Citation List

Non Patent Literature

[0004]

Non Patent Literature 1: WIRESHARK, [online], [Searched on February 25, 2021], Internet <URL: https://www.wireshark.org/>

Non Patent Literature 2: zeek, [online], [Searched on February 25, 2021], Internet <URL: https://zeek.org/>

Summary

[0004A]

It is an object of the present invention to substantially overcome or at least ameliorate one or more of the above disadvantages, or provide a useful alternative.

[0005]

However, none of the Non Patent Literatures can specify an abnormal byte in an abnormal packet.

[0006]

Some embodiments of the present disclosure are intended to provide a technology capable of estimating an abnormal byte in an abnormal packet.

[0006a]

According to one aspect of the present invention, there is provided an estimation apparatus comprising: a conversion unit that converts abnormal packet data into abnormal vector data using a model that converts packet data into vector data in which each byte of the packet data is associated with each vector representing a characteristic of a value of each byte; an extraction unit that extracts normal vector data having a relatively high similarity to the abnormal vector data from among a plurality of pieces of normal vector data obtained by converting a plurality of pieces of normal packet data using the model; and an estimation unit that estimates an abnormal byte in the abnormal packet data from a similarity between a vector corresponding to a byte of the abnormal vector data and a vector corresponding to a byte of the extracted normal vector data, wherein the abnormal packet data comprises the abnormal byte and at least one normal byte.

[0006b]

According to another aspect of the present invention, there is provided a program for causing a computer to function as the estimation apparatus according to the above aspect.

[0006c]

According to another aspect of the present

invention, there is provided an estimation method comprising the steps of: converting, by a computer, abnormal packet data into abnormal vector data using a model that converts packet data into vector data in which each byte of the packet data is associated with each vector representing a characteristic of a value of each byte; extracting, by the computer, normal vector data having a relatively high similarity to the abnormal vector data from among a plurality of pieces of normal vector data obtained by converting a plurality of pieces of normal packet data using the model; and estimating, by the computer, an abnormal byte in the abnormal packet data from a similarity between a vector corresponding to a byte of the abnormal vector data and a vector corresponding to a byte of the extracted normal vector data, wherein the abnormal packet data comprises the abnormal byte and at least one normal byte.

[0007]

An estimation apparatus according to an aspect of the present disclosure includes: a conversion unit that converts abnormal packet data into abnormal vector data using a model that converts packet data into vector data in which each byte of the packet data is associated with each vector representing a characteristic of a value of each byte; an extraction unit that extracts normal vector data

having a relatively high similarity to the abnormal vector data from among a plurality of pieces of normal vector data obtained by converting a plurality of pieces of normal packet data using the model; and an estimation unit that estimates an abnormal byte in the abnormal packet data from a similarity between a vector corresponding to each byte of the abnormal vector data and a vector corresponding to each byte of the extracted normal vector data.

[0008]

An estimation method according to an aspect of the present disclosure includes the steps of: converting, by a computer, abnormal packet data into abnormal vector data using a model that converts packet data into vector data in which each byte of the packet data is associated with each vector representing a characteristic of a value of each byte; extracting, by the computer, normal vector data having a relatively high similarity to the abnormal vector data from among a plurality of pieces of normal vector data obtained by converting a plurality of pieces of normal packet data using the model; and estimating, by the computer, an abnormal byte in the abnormal packet data from a similarity between a vector corresponding to each byte of the abnormal vector data and a vector corresponding to each byte of the extracted normal vector data.

[0009]

2021432832 04 Sep 2024

An aspect of the present disclosure is a program for causing a computer to function as the above estimation apparatus.

[0010]

According to some embodiments of the present disclosure, it is possible to provide a technology capable of estimating an abnormal byte in an abnormal packet.

Brief Description of Drawings

[0011]

[Fig.1] Fig. 1 is a diagram for explaining functional blocks of an estimation apparatus according to an embodiment of the present invention.

[Fig.2] Fig. 2 is a diagram for explaining an example of data converted by a model.

[Fig.3] Fig. 3 is a flowchart illustrating an example

of processing of an estimation method.

[Fig.4] Fig. 4 is a diagram for explaining each device of an evaluation system of an estimation apparatus.

[Fig.5] Fig. 5 is a diagram for explaining an example of a packet obtained in the evaluation system.

[Fig.6] Fig. 6 is a diagram for explaining an example of a similarity matrix obtained in the evaluation system.

[Fig.7] Fig. 7 is a diagram for explaining a hardware configuration of a computer to be used in the estimation apparatus.

Description of Embodiments

[0012]

Hereinafter, an embodiment of the present invention will be described with reference to the drawings. In the drawings, the same parts are denoted by the same reference signs, and description thereof is omitted.

[0013]

(Estimation Apparatus)

An estimation apparatus 1 according to an embodiment of the present invention will be described with reference to Fig. 1. When an abnormal packet is inputted, the estimation apparatus 1 estimates and outputs an abnormal byte in the abnormal packet. The estimation apparatus 1 compares an abnormal packet determined to be abnormal by

another system with a normal packet determined to be normal by the other system, and estimates an abnormal byte in the inputted abnormal packet. For example, a normal packet and an abnormal packet are each collected in a communication network of one operation technology. Another system may determine whether a packet is normal or abnormal by an arbitrary method, and the determination method is not limited in the embodiment of the present invention.

[0014]

The estimation apparatus 1 includes each data of model data 11, a normal vector data group 12, abnormal packet data 15, abnormal vector data 16, normal vector data 17, and an abnormal byte 18, and each function of a conversion unit 21, a generation unit 22, an extraction unit 23, and an estimation unit 24. Each data is stored in a memory 902 or a storage 903. Each function is implemented by a CPU 901.

[0015]

The model data 11 specifies a model that converts packet data into vector data. The vector data associates each byte of packet data with each vector representing a characteristic of a value of each byte. The model data 11 is generated by learning the value of each byte of a plurality of pieces of normal packet data of the normal vector data group 12 by the generation unit 22 (which will

be described later). The characteristic of the value of each byte is calculated by comparison with the value of each byte of a plurality of pieces of normal packet data.

[0016]

The model data 11 specifies a model that converts each byte of the inputted packet data into a vector having an appropriate fixed length in consideration of a positional relationship of each byte and the like. Here, the vector having an appropriate fixed length means a vector with which the abnormal byte 18 can be estimated by comparing the abnormal vector data 16 and the normal vector data 17 in the estimation unit 24 (which will be described later). For example, as illustrated in Fig. 2, it is assumed that there is packet data having a fixed length such as a value of a first byte “2e”, a value of a second byte “3f”, a value of a third byte “00”...,. Each byte of the packet data is converted into a 784-dimensional vector by the model. In the example illustrated in Fig. 2, the model converts each byte of the packet data into a 784-dimensional vector representing a characteristic of a value of each byte.

[0017]

The model data 11 is generated by bidirectional encoder representations from transformers (BERT), for example. BERT is a natural language processing model. In

the embodiment of the present invention, each byte of packet data is regarded as one word. The packet data is converted into vector data by a model generated using BERT.

[0018]

The normal vector data group 12 includes a plurality of pieces of normal vector data. The normal vector data is data obtained by converting normal packet data using a model specified by the model data 11. The normal packet data is determined to be normal in another system. The normal vector data group 12 is referred to when the generation unit 22 generates the model data 11 or when the extraction unit 23 extracts the normal vector data 17 similar to the abnormal vector data 16. Both the generation unit 22 and the extraction unit 23 may refer to a plurality of pieces of normal vector data included in the normal vector data group 12. Alternatively, a plurality of pieces of normal vector data included in the normal vector data group 12 may be divided into a plurality of groups, one group may be referred to by the generation unit 22, and another group may be referred to by the extraction unit 23.

[0019]

The abnormal packet data 15 is data of a packet specified as an abnormal packet in another system. The estimation apparatus 1 estimates an abnormal byte 18 for one piece of abnormal packet data 15.

[0020]

The abnormal vector data 16 is data obtained by converting the abnormal packet data 15 by the model specified by the model data 11. The abnormal vector data 16 associates an identifier of a position of each byte of the abnormal packet data 15 with each vector representing a characteristic of a value of each byte.

[0021]

The normal vector data 17 is data having a relatively high similarity to the abnormal vector data 16 among a plurality of pieces of normal vector data included in the normal vector data group 12. The normal vector data 17 is normal vector data having the highest similarity to the abnormal vector data 16 among a plurality of pieces of normal vector data included in the normal vector data group 12. Alternatively, the normal vector data 17 is one of a predetermined number of pieces of normal vector data having high similarity.

[0022]

The abnormal byte 18 is data that specifies a byte, which is estimated to be abnormal, among bytes of the abnormal packet data 15. For example, the abnormal byte 18 is specified in the order in which the position of each byte of the abnormal packet data 15 is counted from the head.

[0023]

The conversion unit 21 converts the abnormal packet data 15 into abnormal vector data 16 using the model specified by the model data 11. For example, as illustrated in Fig. 2, the conversion unit 21 converts the value of each byte of the abnormal packet data 15 into a 784-dimensional vector. The conversion unit 21 associates the position of each byte of the abnormal packet data 15 with the 784-dimensional vector obtained by conversion from the byte, and outputs the abnormal vector data 16.

[0024]

The generation unit 22 learns the value of each byte of a plurality of pieces of normal packet data of the normal vector data group 12 and generates a model specified by the model data 11. The model converts the packet data into vector data that associates each byte of the packet data with each vector representing a characteristic of the value of each byte. The generation unit 22 generates a model according to BERT, for example. The generation unit 22 may perform preliminary learning about the characteristic of the value of each byte in the normal packet data by solving an auxiliary task such as a masked language model (MLM) or a next sentence prediction (NSP). MLM predicts the values of missing bytes in packets in which a plurality of bytes are missing. The NSP determines

whether two pieces of packet data are consecutive packets or not. The generation unit 22 specifies validity of data in a packet and validity of consecutive packets by using these auxiliary tasks, and the generation unit 22 generates a model that specifies normal vector data. The auxiliary tasks described herein are merely an example, and the generation unit 22 may learn by solving other auxiliary tasks.

[0025]

The extraction unit 23 extracts normal vector data having a relatively high similarity to the abnormal vector data 16 from among a plurality of pieces of normal vector data of the normal vector data group 12. The extraction unit 23 regards the extracted normal vector data as the normal vector data 17.

[0026]

Having a relatively high similarity means that the similarity between the abnormal vector data 16 and certain normal vector data is higher than the similarity between the abnormal vector data 16 and the other normal vector data. The extraction unit 23 may extract normal vector data having the highest similarity to the abnormal vector data 16. Alternatively, the extraction unit 23 may extract one piece of normal vector data from among a plurality of pieces of normal vector data of a predetermined number or a

predetermined ratio having a high similarity to the abnormal vector data 16.

[0027]

The extraction unit 23 calculates a similarity between the abnormal vector data 16 and each normal vector data of the normal vector data group 12. The extraction unit 23 may calculate a similarity to a part of normal vector data in the normal vector data group 12. For example, a part of the normal vector data is a plurality of pieces of normal vector data obtained by extracting a plurality of pieces of representative packet data from among a plurality of pieces of normal packet data by using MMD-Critic (maximum mean discrepancy (MMD)) and converting each piece of the extracted representative packet data by using a model. Alternatively, a part of the normal vector data is a plurality of pieces of normal vector data obtained by extracting normal packet data having the same packet length as the abnormal packet data 15 from among a plurality of pieces of normal packet data and converting each piece of the extracted normal packet data by using a model.

[0028]

In a case where the model is BERT, the extraction unit 23 may use BERT Score as the similarity. Alternatively, the extraction unit 23 may calculate a

similarity between the vector of the abnormal vector data 16 and the vector of the normal vector data for each byte of the abnormal vector data 16, and calculate a similarity between the abnormal vector data 16 and the normal vector data from the similarity calculated for each byte. As the similarity between vectors of each byte, a Cosine similarity may be used. The similarity between the abnormal vector data 16 and the normal vector data 17 is, for example, an average of similarities calculated for each byte. At this time, in a case where the number of vectors of the abnormal vector data 16 is different from the number of vectors of the normal vector data 17, the similarity may be calculated according to the smaller number of vectors. Note that the number of vectors of each vector data is the number of bytes of the packet data before conversion.

[0029]

The estimation unit 24 estimates an abnormal byte 18 in the abnormal packet data 15 from the similarity between the vector corresponding to each byte of the abnormal vector data 16 and the vector corresponding to each byte of the extracted normal vector data 17.

[0030]

The estimation unit 24 calculates a Cosine similarity matrix illustrated in Fig. 6 between each vector included in the abnormal vector data 16 and each vector

included in the normal vector data 17. The (n, m) component of the Cosine similarity matrix is the Cosine similarity between the vector corresponding to the n-th byte of the abnormal vector data 16 and the vector corresponding to the m-th byte of the normal vector data 17.

[0031]

For example, in a case where the highest similarity among the similarities between the vector corresponding to the predetermined byte of the abnormal packet data 15 and the vector corresponding to each byte of the extracted normal vector data 17 is lower than a predetermined threshold, the estimation unit 24 estimates the predetermined byte as the abnormal byte 18. Whether the i-th byte of the abnormal packet data 15 is an abnormal byte or not is estimated as follows. The m is a packet length of the normal packet data. The estimation unit 24 focuses on the respective components of the (i, 1) component, the (i, 2) component, the (i, 3) component,..., and the (i, m) component of the Cosine similarity matrix calculated as above. The estimation unit 24 estimates that the i-th byte is the abnormal byte 18 when the component having the highest Cosine similarity among the official texts is equal to or less than a certain threshold.

[0032]

In a case where the number of bytes of the abnormal packet data 15 is the same as the number of bytes of the packet data before conversion of the normal vector data 17, vectors corresponding to the same byte of the abnormal packet data 15 and the normal vector data 17 may be compared with each other. For example, in a case where the similarity between the vector data corresponding to the i-th byte of the abnormal packet data 15 and the vector data corresponding to the i-th byte of the normal packet data is lower than a predetermined threshold when estimating whether the i-th byte of the abnormal packet data 15 is an abnormal byte or not, the estimation unit 24 estimates the i-th byte of the abnormal packet data 15 as an abnormal byte.

[0033]

The threshold for the estimation unit 24 to determine whether the byte is an abnormal byte or not may be, for example, a fixed value such as 0.5. Alternatively, the threshold may be specified by predetermined calculation. For example, a plurality of pairs of two normal packets similar to each other may be extracted, and the threshold may be specified from the lowest similarity among the similarities of the respective vectors of two normal packets corresponding to a predetermined byte.

[0034]

An estimation method performed by the estimation apparatus 1 according to the embodiment of the present invention will be described with reference to Fig. 3.

[0035]

In step S1, the estimation apparatus 1 converts the abnormal packet data 15 into abnormal vector data 16. In step S2, the estimation apparatus 1 extracts normal vector data 17 similar to the abnormal vector data 16 obtained by conversion in step S1 from the normal vector data group 12.

[0036]

The processing of steps S3 to S5 is repeated for each vector of the abnormal vector data 16, in other words, each vector corresponding to each byte of the abnormal packet data 15.

[0037]

The processing of step S3 is repeated for each vector of the normal vector data 17 extracted in step S2. In step S3, the estimation apparatus 1 calculates the similarity between the processing target vector of the abnormal vector data 16 and the processing target vector of the normal vector data 17. When the similarity is calculated, the processing proceeds to step S4.

[0038]

In step S4, the estimation apparatus 1 determines whether the highest similarity among the plurality of

similarities calculated for the processing target vector of the abnormal vector data 16 and each vector of the normal vector data 17 is lower than a predetermined threshold or not. When the highest similarity is higher than the predetermined threshold, the estimation apparatus 1 estimates that the processing target vector of the abnormal vector data 16 does not correspond to an abnormal byte. The estimation apparatus 1 processes step S3 for the next processing target vector.

[0039]

When the highest similarity is lower than the predetermined threshold, the estimation apparatus 1 estimates that the processing target vector of the abnormal vector data 16 corresponds to an abnormal byte. In step S6, the estimation apparatus 1 outputs a byte corresponding to the processing target vector of the abnormal vector data 16 as an abnormal byte 18.

[0040]

When the processing of steps S3 to S5 ends for each vector of the abnormal vector data 16, the estimation apparatus 1 ends the processing.

[0041]

Evaluation of the estimation apparatus 1 will be described with reference to Figs. 4 to 6. In the evaluation of the estimation apparatus 1, a virtual

evaluation system is used.

[0042]

As illustrated in Fig. 4, the evaluation system controls movement of loads B1 and B2 by arranging four belt conveyors C1 to C4 in a rectangular shape and using a programmable logic controller (PLC) (not shown). Each device illustrated in Fig. 4 transmits a packet for notifying a PLC of a state or receives a packet for designating a drive content from the PLC, according to a Modbus/TCP protocol or the like. In the normal state, the PLC drives pushers P1 to P4 according to the detection situation of sensors S1 to S4, and thus the belt conveyors C1 to C4 carry the loads B1 and B2 counterclockwise at a constant speed. The speed of the belt conveyors is sequentially monitored by the PLC. When the speed of the belt conveyors exceeds the constant speed, the PLC issues an emergency stop command to each device illustrated in Fig. 4, and each device stops.

[0043]

For example, the load B1 moves on the belt conveyor C1. At this time, the belt conveyor C1 transmits a packet for giving a notification of the moving speed of the belt to the PLC. When the load B1 comes into contact with a laser beam emitted from the sensor S1, the sensor S1 transmits a packet for giving a notification that the load

has arrived to the PLC. Note that the laser beam is shown by an alternate long and short dash line in the example illustrated in Fig. 4. Upon receiving the packet, the PLC transmits a packet for turning on the pusher P1. The pusher P1 extends from the box according to the received packet and carries the load B1 to the belt conveyor C2. When the load no longer comes into contact with a laser beam emitted from the sensor S1, the sensor S1 transmits a packet for giving a notification that there is no load to the PLC. Upon receiving the packet, the PLC transmits a packet for turning off the pusher P1. The pusher P1 is shortened and accommodated in the box according to the received packet. By repeating such processing by each device, the load B1 moves counterclockwise on the belt conveyors illustrated in Fig. 4. Similarly, the load B2 moves counterclockwise on the belt conveyors illustrated in Fig. 4.

[0044]

The PLC collects normal packet data when each device illustrated in Fig. 4 operates normally. The generation unit 22 learns a plurality of pieces of normal packet data collected by the PLC to generate the model data 11. In the evaluation system, the extraction unit 23 refers to a plurality of pieces of normal vector data obtained from conversion from each normal packet data collected by the

PLC. Moreover, BERT Score F1 is used as a measure of similarity.

[0045]

An abnormal state is generated by manually moving the belt conveyors quickly such that the speed becomes an abnormal value. A packet for giving a notification of the speed of the belt conveyors in this abnormal state is inputted to the PLC as abnormal packet data 15.

[0046]

The extraction unit 23 extracts normal vector data most similar to the abnormal vector data 16 obtained by conversion from the abnormal packet data 15. Fig. 5 illustrates comparison between the abnormal packet data 15 and the normal packet data before conversion of the normal vector data extracted by the extraction unit 23.

[0047]

In Fig. 5, the communication ID is set in the first byte and the second byte. The communication ID is an identifier that specifies a packet transmitted and received in the system illustrated in Fig. 4. In the 11th byte, the speed of the belt conveyor is set. In the example illustrated in Fig. 5, the values of the abnormal packet and the normal packet are different in the first byte, the second byte, and the 11th byte, but the values in the other bytes are the same. It can be seen that the extraction

unit 23 has extracted normal vector data most similar to the abnormal vector data 16.

[0048]

Fig. 6 is a similarity matrix between vectors of respective bytes of an abnormal packet and a normal packet. It can be seen from Fig. 6 that high similarities are arranged diagonally. However, the similarities of comparison between the first bytes, the second bytes, and the 11th bytes on the diagonal have low values. It is considered that the first byte, the second byte, or the 11th byte of the abnormal packet may be an abnormal byte.

[0049]

On the other hand, as a result of comparing two pieces of normal vector data obtained by conversion from two normal packets similar to each other, the lowest similarity among the similarities obtained by comparing vectors corresponding to the same byte was 0.91. This 0.91 is used as a threshold for detecting an abnormal byte.

[0050]

Since the similarity of each of the first byte and the second byte is larger than 0.91, the estimation unit 24 estimates that the first byte and the second byte are not abnormal bytes. In the first byte and the second byte, since different communication IDs are set for each packet, a similarity higher than the threshold is calculated even

if different values are set for the normal packet and the abnormal packet.

[0051]

On the other hand, since the similarity at the 11th byte is 0.827 and is smaller than 0.91, the estimation unit 24 estimates the 11th byte as an abnormal byte. In the 11th byte, the speed of the belt conveyor is set. This estimation performed by the estimation unit 24 also coincides with a situation in which an abnormal state has been generated by manually moving the belt conveyors quickly.

[0052]

The estimation apparatus 1 according to the embodiment of the present invention can estimate the abnormal byte 18 in the abnormal packet data 15. As a result, the estimation apparatus 1 can precisely analyze the content of the payload. For example, by introducing the estimation apparatus 1 into a communication network or the like of an operational technology in an industrial system, a building system, or the like, it is possible to detect packets without overlooking even a small amount of unauthorized rewriting such as one byte.

[0053]

The estimation apparatus 1 according to the present embodiment described above is, for example, a general-

purpose computer system including the central processing unit (CPU, processor) 901, the memory 902, the storage 903 (hard disk drive (HDD) or solid state drive (SSD)), a communication device 904, an input device 905, and an output device 906. In this computer system, each function of the estimation apparatus 1 is implemented by the CPU 901 executing a program loaded on the memory 902.

[0054]

Note that the estimation apparatus 1 may be implemented by one computer or may be implemented by a plurality of computers. Moreover, the estimation apparatus 1 may be a virtual machine that is implemented by a computer.

[0055]

The program for the estimation apparatus 1 can be stored in a computer-readable recording medium such as an HDD, an SSD, a universal serial bus (USB) memory, a compact disc (CD), or a digital versatile disc (DVD), or can be distributed via a network.

[0056]

Note that the present invention is not limited to the above embodiment, and various modifications can be made within the scope of the gist of the present invention.

Reference Signs List

[0057]

1	Estimation apparatus
11	Model data
12	Normal vector data group
15	Abnormal packet data
16	Abnormal vector data
17	Normal vector data
18	Abnormal byte
21	Conversion unit
22	Generation unit
23	Extraction unit
24	Estimation unit
901	CPU
902	Memory
903	Storage
904	Communication device
905	Input device
906	Output device

2021432832 04 Sep 2024

Claims

[Claim 1]

An estimation apparatus comprising:

a conversion unit that converts abnormal packet data into abnormal vector data using a model that converts packet data into vector data in which each byte of the packet data is associated with each vector representing a characteristic of a value of each byte;

an extraction unit that extracts normal vector data having a relatively high similarity to the abnormal vector data from among a plurality of pieces of normal vector data obtained by converting a plurality of pieces of normal packet data using the model; and

an estimation unit that estimates an abnormal byte in the abnormal packet data from a similarity between a vector corresponding to a byte of the abnormal vector data and a vector corresponding to a byte of the extracted normal vector data, wherein the abnormal packet data comprises the abnormal byte and at least one normal byte.

[Claim 2]

The estimation apparatus according to claim 1,

wherein the model is generated by learning a value of each byte of a plurality of pieces of normal packet data.

[Claim 3]

The estimation apparatus according to claim 1,

wherein the extraction unit calculates a similarity between a vector of the abnormal vector data and a vector of the normal vector data for each byte of the abnormal vector data to calculate a similarity between the abnormal vector data and the normal vector data from the similarity calculated for each byte.

[Claim 4]

The estimation apparatus according to claim 1,

wherein in a case where a highest similarity among similarities between a vector corresponding to a predetermined byte of the abnormal packet data and a vector corresponding to each byte of the extracted normal vector data is lower than a predetermined threshold, the estimation unit estimates the predetermined byte as the abnormal byte.

[Claim 5]

An estimation method comprising the steps of:

converting, by a computer, abnormal packet data into abnormal vector data using a model that converts packet data into vector data in which each byte of the packet data is associated with each vector representing a characteristic of a value of each byte;

extracting, by the computer, normal vector data having a relatively high similarity to the abnormal vector

2021432832 04 Sep 2024

data from among a plurality of pieces of normal vector data obtained by converting a plurality of pieces of normal packet data using the model; and

estimating, by the computer, an abnormal byte in the abnormal packet data from a similarity between a vector corresponding to a byte of the abnormal vector data and a vector corresponding to a byte of the extracted normal vector data, wherein the abnormal packet data comprises the abnormal byte and at least one normal byte.

[Claim 6]

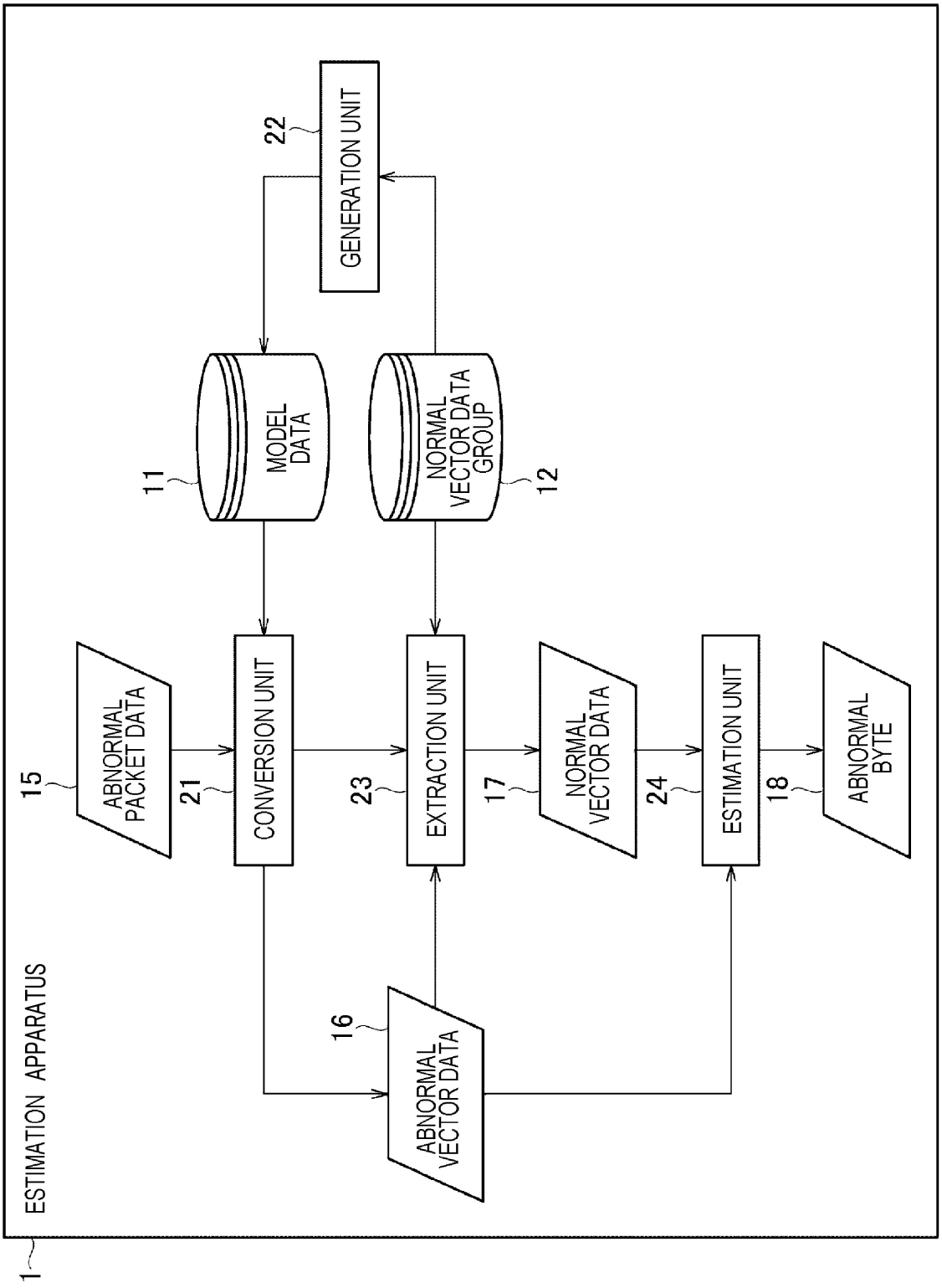
A program for causing a computer to function as the estimation apparatus according to any one of claims 1 to 4.

Nippon Telegraph and Telephone Corporation

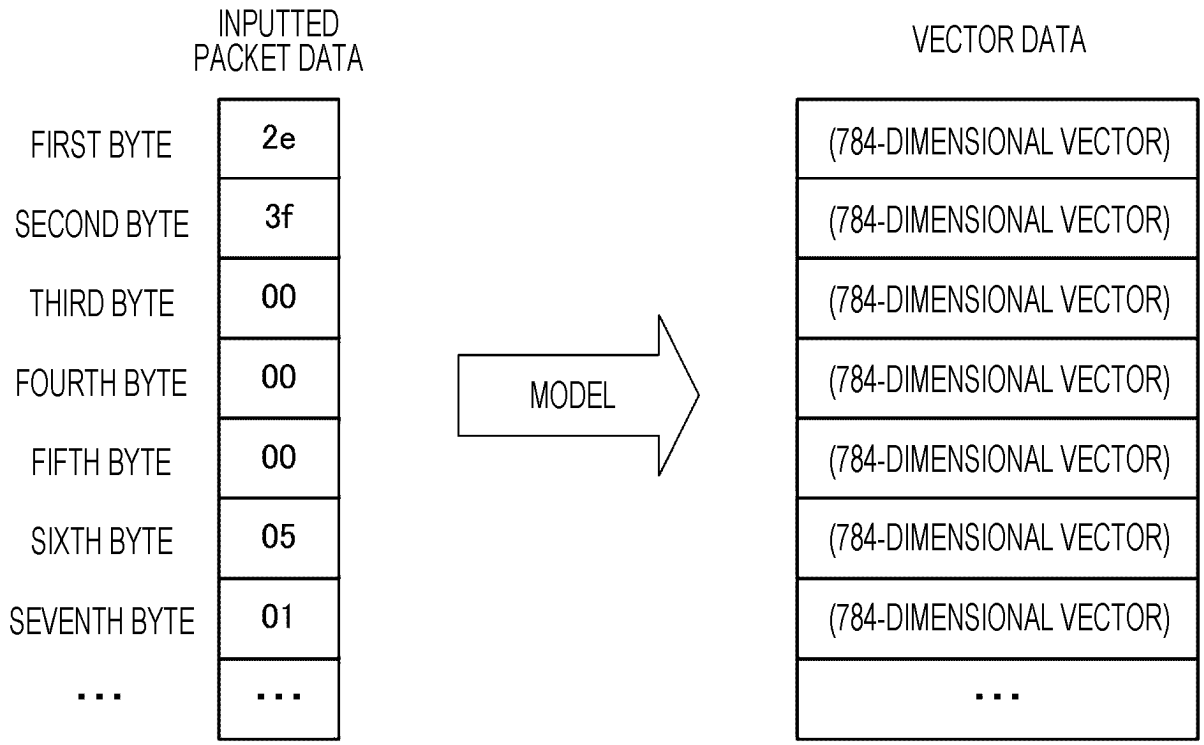
Patent Attorneys for the Applicant/Nominated Person

SPRUSON & FERGUSON

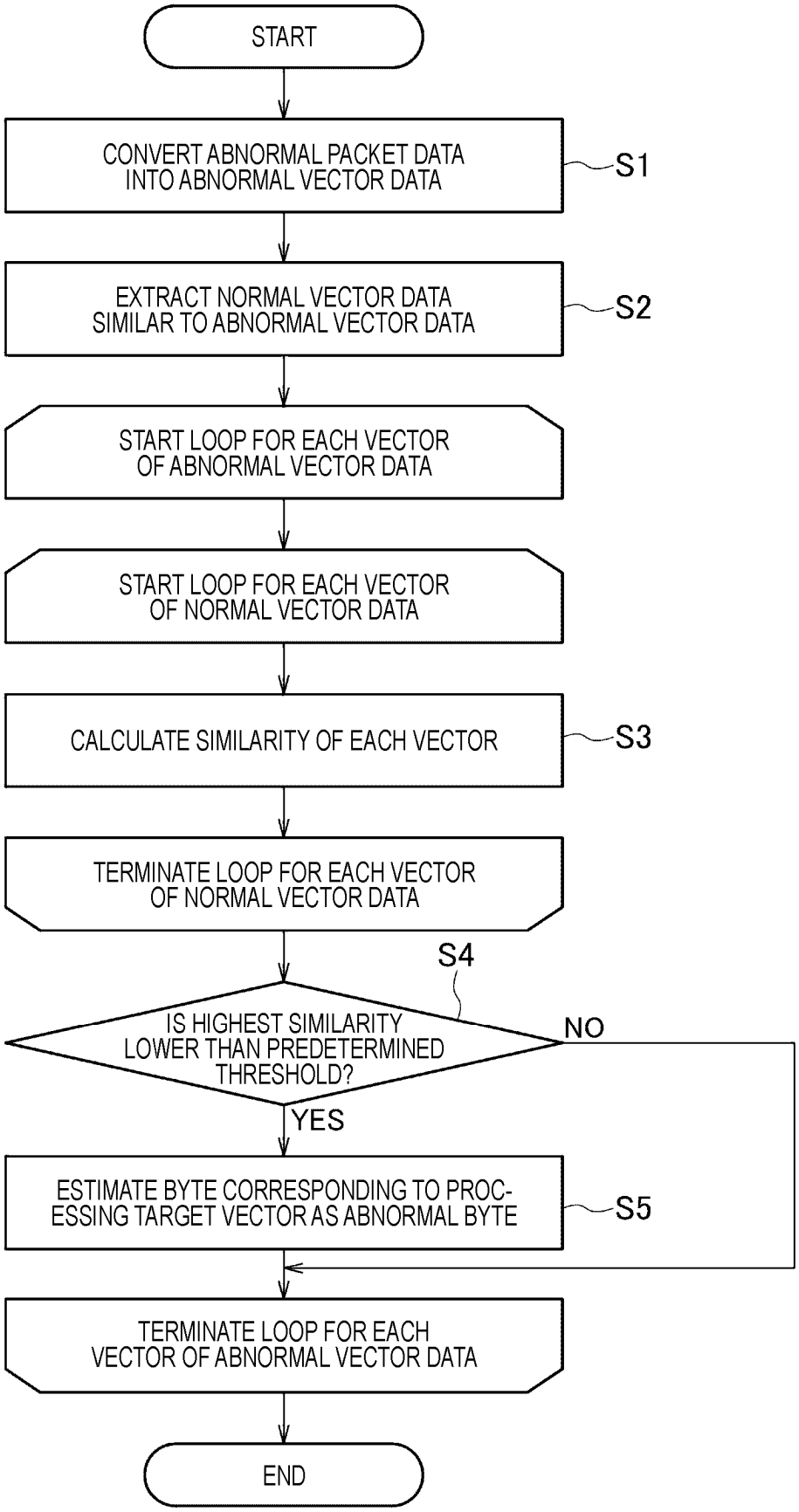
[Fig. 1]


ESTIMATION APPARATUS
1
GENERATION UNIT
22
MODEL DATA
11
NORMAL VECTOR DATA GROUP
12
ABNORMAL PACKET DATA
15
CONVERSION UNIT
21
EXTRACTION UNIT
23
NORMAL VECTOR DATA
17
ESTIMATION UNIT
24
ABNORMAL BYTE
18
ABNORMAL VECTOR DATA
16

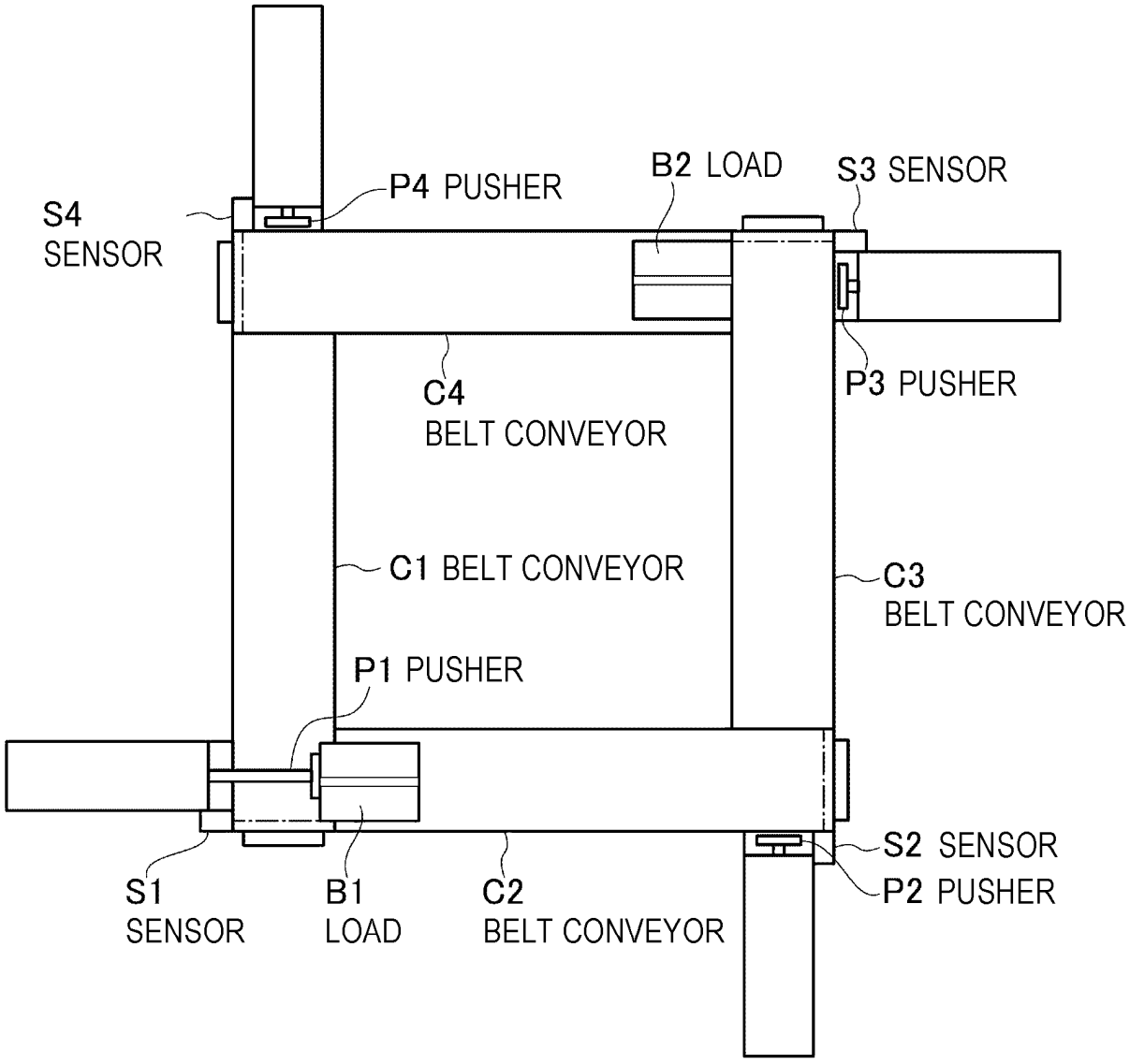
[Fig. 2]


INPUTTED PACKET DATA
FIRST BYTE
2e
SECOND BYTE
3f
THIRD BYTE
00
FOURTH BYTE
00
FIFTH BYTE
00
SIXTH BYTE
05
SEVENTH BYTE
01
...
...
MODEL
VECTOR DATA
(784-DIMENSIONAL VECTOR)
(784-DIMENSIONAL VECTOR)
(784-DIMENSIONAL VECTOR)
(784-DIMENSIONAL VECTOR)
(784-DIMENSIONAL VECTOR)
(784-DIMENSIONAL VECTOR)
(784-DIMENSIONAL VECTOR)
...

[Fig. 3]


START
CONVERT ABNORMAL PACKET DATA INTO ABNORMAL VECTOR DATA
S1
EXTRACT NORMAL VECTOR DATA SIMILAR TO ABNORMAL VECTOR DATA
S2
START LOOP FOR EACH VECTOR OF ABNORMAL VECTOR DATA
START LOOP FOR EACH VECTOR OF NORMAL VECTOR DATA
CALCULATE SIMILARITY OF EACH VECTOR
S3
TERMINATE LOOP FOR EACH VECTOR OF NORMAL VECTOR DATA
S4
IS HIGHEST SIMILARITY LOWER THAN PREDETERMINED THRESHOLD?
NO
YES
ESTIMATE BYTE CORRESPONDING TO PROCESSING TARGET VECTOR AS ABNORMAL BYTE
S5
TERMINATE LOOP FOR EACH VECTOR OF ABNORMAL VECTOR DATA
END

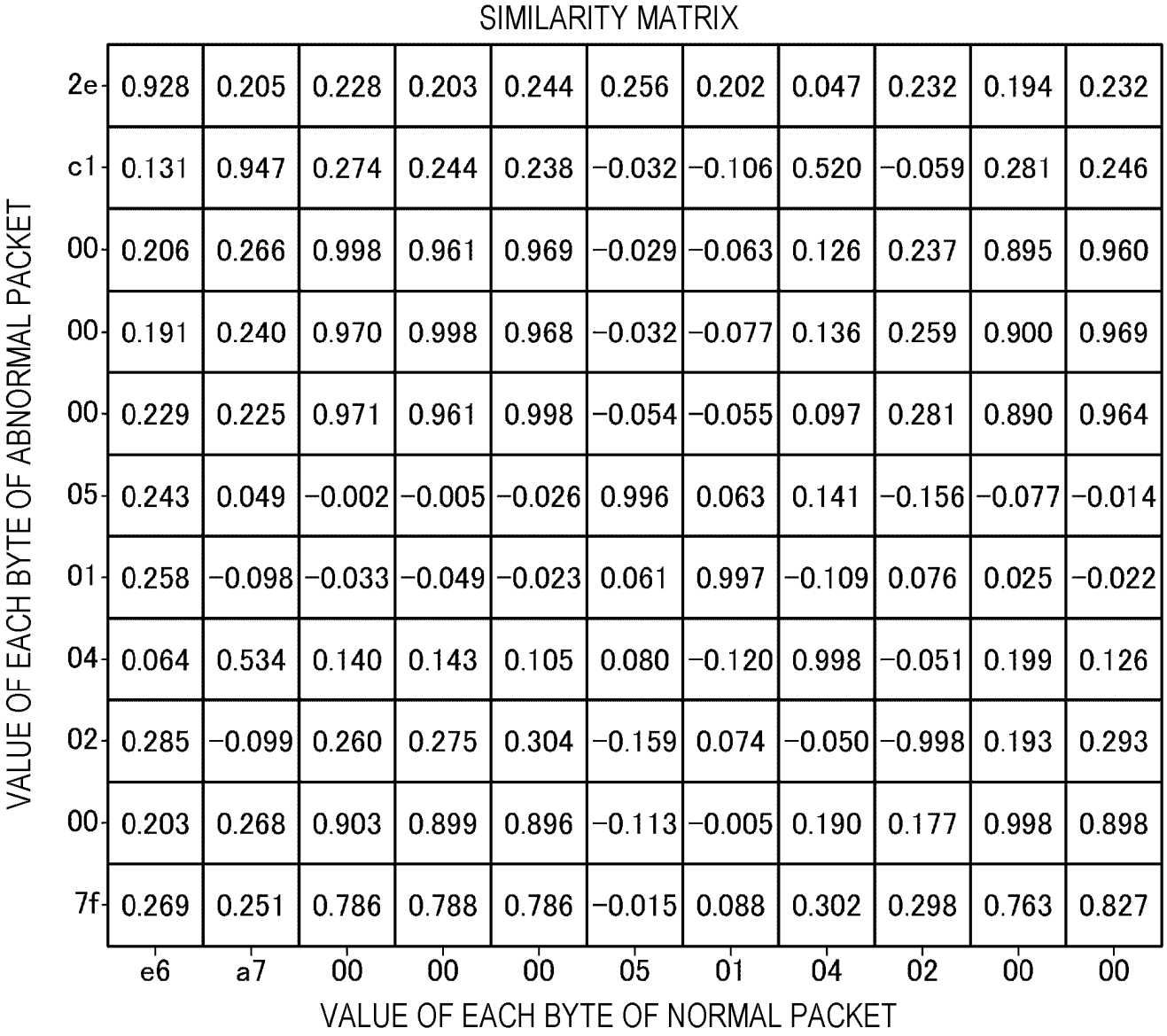
[Fig. 4]


S4
SENSOR
P4 PUSHER
B2 LOAD
S3 SENSOR
C4
BELT CONVEYOR
P3 PUSHER
C1 BELT CONVEYOR
C3
BELT CONVEYOR
P1 PUSHER
S2 SENSOR
P2 PUSHER
S1
SENSOR
B1
LOAD
C2
BELT CONVEYOR

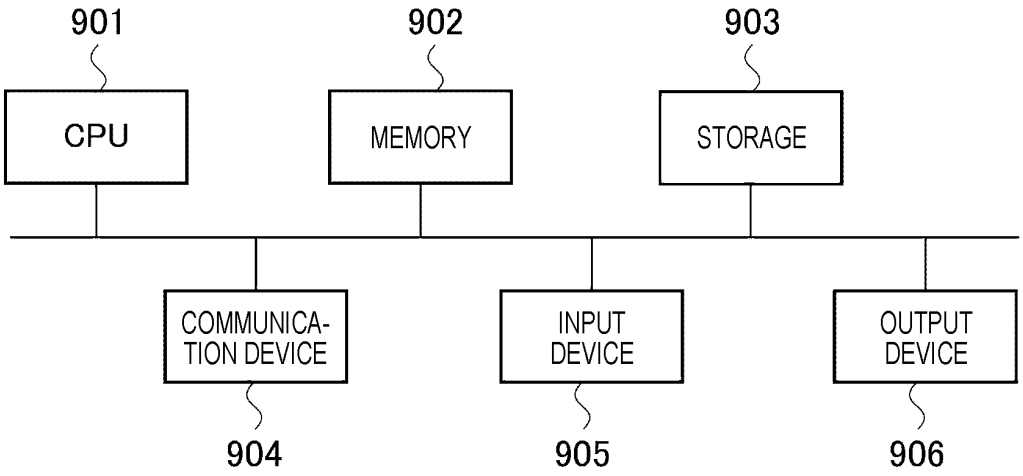
[Fig. 5]

BYTE	1	2	3	4	5	6	7	8	9	10	11
ABNORMAL PACKET	2e	3f	00	00	00	06	01	04	02	00	7f
NORMAL PACKET	e6	a7	00	00	00	06	01	04	02	00	00

[Fig. 6]


SIMILARITY MATRIX
VALUE OF EACH BYTE OF ABNORMAL PACKET
VALUE OF EACH BYTE OF NORMAL PACKET
2e 0.928 0.205 0.228 0.203 0.244 0.256 0.202 0.047 0.232 0.194 0.232
c1 0.131 0.947 0.274 0.244 0.238 −0.032 −0.106 0.520 −0.059 0.281 0.246
00 0.206 0.266 0.998 0.961 0.969 −0.029 −0.063 0.126 0.237 0.895 0.960
00 0.191 0.240 0.970 0.998 0.968 −0.032 −0.077 0.136 0.259 0.900 0.969
00 0.229 0.225 0.971 0.961 0.998 −0.054 −0.055 0.097 0.281 0.890 0.964
05 0.243 0.049 −0.002 −0.005 −0.026 0.996 0.063 0.141 −0.156 −0.077 −0.014
01 0.258 −0.098 −0.033 −0.049 −0.023 0.061 0.997 −0.109 0.076 0.025 −0.022
04 0.064 0.534 0.140 0.143 0.105 0.080 −0.120 0.998 −0.051 0.199 0.126
02 0.285 −0.099 0.260 0.275 0.304 −0.159 0.074 −0.050 −0.998 0.193 0.293
00 0.203 0.268 0.903 0.899 0.896 −0.113 −0.005 0.190 0.177 0.998 0.898
7f 0.269 0.251 0.786 0.788 0.786 −0.015 0.088 0.302 0.298 0.763 0.827
e6 a7 00 00 00 05 01 04 02 00 00

[Fig. 7]


901
902
903
CPU
MEMORY
STORAGE
COMMUNICA-
TION DEVICE
INPUT
DEVICE
OUTPUT
DEVICE
904
905
906