Time-tunnel: 3D Visualization Tool and Its Aspects as 3D Parallel Coordinates

Yoshihiro Okada
ICER(Innovation Center for Educational Resources) of Kyushu University Library, Cybersecurity Center and Graduate School of ISEE, Kyushu University, Fukuoka, Japan
okada@inf.kyushu-u.ac.jp

Abstract—**This paper treats a 3D visualization tool called *Time-tunnel*, especially describes its aspects as 3D Parallel Coordinates by showing its actual visualization examples. Originally, *Time-tunnel* is a multidimensional data visualization tool and it was extended to support Parallel Coordinates called *PCTT*(Parallel Coordinates version of *Time-tunnel*). Furthermore, as its aspects of 3D Parallel Coordinates, 2Dto2D visualization functionality was added. Although *PCTT* can visualize network data because IP packets consist of many attributes and such multiple-attributes data can be visualized using Parallel Coordinates, 2Dto2D visualization functionality can more effectively visualize patterns of IP packets that seem network attacks. The authors have already proposed the combinatorial use of *PCTT* and 2Dto2D visualization for the intrusion detection of the Internet. This paper also introduces Spline Parallel Coordinates representation as one of the new features of *PCTT*. The authors also proposed the use of *PCTT* for learning analytics by visualizing leaners' learning activity data and introduced 3D mode into *PCTT* to visualize each learner's learning pattern more efficiently. This 3D mode is regarded as 3D Parallel Coordinates. However, because such 3D mode was not enough to distinguish each learner's leaning pattern, the authors implemented more effective 3D mode, and clarify the usefulness of the new 3D mode by showing visualization results.**

Keywords- 3D visualization, Parallel Coordinates, Time-tunnel, network traffic data, learning activity data.

I. INTRODUCTION

This paper treats a 3D visualization tool called *Time-tunnel* [1]. Originally, *Time-tunnel* was implemented for visualizing time-series numerical data, and also extended for visualizing multidimensional (multiple attributes) data like Parallel Coordinates [2]. This is called Parallel Coordinates version of *Time-tunnel* (*PCTT*) [3]. *PCTT* visualizes huge number of multidimensional data records as individual charts in a 3D space. Those charts are displayed on a rectangular plane and the user easily puts more than one different planes overlapped together to compare their data records represented as charts in order to recognize the similarity or the difference among them. Simultaneously, a radar chart among those data on any attribute is displayed in the same 3D space to recognize the similarity and the correlation among them. In this way, the user can visually analyze huge number of multidimensional data through interactive manipulations on a computer screen.

One of the examples using *PCTT* is for the visualization of network data [4, 5] because IP packets data have many attributes and such multiple attribute data can be visualized using Parallel Coordinates. Furthermore, we introduced 2Dto2D visualization functionality as an aspect of 3D Parallel Coordinates to *PCTT* for the intrusion detection of network data by efficiently visualizing patterns of IP packets data that seem network attacks. 2Dto2D visualization functionality displays multiple lines those represent four dimensional (four attributes) data drawn from one (2D of two attributes) plane to the other (2D of the other two attributes) plane. Using 2Dto2D visualization, it is easy to understand relationships of four attributes of each data. Network attacks have a certain access pattern strongly related to the four attributes of IP packets data, i.e., source IP, destination IP, source Port and destination Port. So, 2Dto2D visualization is useful for detecting such access patterns. In this paper, we show several network attack patterns actually visualized using *PCTT* with 2Dto2D visualization for the intrusion detection. In this paper, we also introduce Spline Parallel Coordinates representation as one of the new features of *PCTT*.

Another visualization example using *PCTT* is for learning analytics by visualizing learners' learning activity data [6]. For visualizing each learner's learning pattern more clearly, we introduced 3D mode as another aspect of 3D Parallel Coordinates into *PCTT*. However, this 3D mode is not enough so we implemented more effective 3D mode, and clarify its usefulness by showing visualization results.

The remainder of this paper is organized as follows. First of all, Section 2 describes related work and points out the difference of our tool from the others. Next, we explain details of *PCTT* and its aspects as 3D Parallel Coordinates in Section 3. Then, Sections 4 and 5 present network data-analysis examples and learning analytics examples, respectively. Finally, we conclude the paper in Section 6.

II. RELATED WORK

Our *PCTT* visualizes multiple charts like Parallel Coordinates on one individual rectangular plane and it originally provides multiple rectangular planes in a 3D space. So, even if the user has a huge amount of data records, he/she can analyze them by separating into several groups using multiple rectangular planes to recognize the similarity or the difference among those data visually and interactively. This is one of the advantages of our *PCTT*. Another popular data analysis method beside Parallel Coordinates is based on star chart or radar chart. Elena Fanea, et al proposed a visualization tool that has combined feature of Parallel Coordinates and Star Glyphs [7]. Our *PCTT* also has

978-1-5386-7202-0/18/$31.00 ©2018 IEEE
DOI 10.1109/iV.2018.00019

combinatorial features of Parallel Coordinates and star chart (radar chart) visualization tool with interactive interfaces.

As visualization tools of network data for the intrusion detection, there are many visualization tools those are referred in our paper [4, 5]. As one of the aspects as 3D Parallel Coordinates, our *PCTT* provides 2Dto2D visualization functionality. Its idea was derived from the visualization tool called nicter Cube [8]. As researches on 3D Parallel Coordinates, there are papers [9-14]. Our 3D Parallel Coordinates is similar to them. However, it has different aspects from them.

III. Parallel coordinates version of Time-tunnel

In this section, we describe the system configuration of *PCTT* (Parallel Coordinates version of Time-tunnel) and its components, and explain how *PCTT* works for the analysis of multidimensional data. In addition, we introduce 2Dto2D visualization and 3D mode functionalities as aspects of 3D Parallel Coordinates.

A. System configuration of Time-tunnel

PCTT was developed using *IntelligentBox* [15], which is a component-based visual and interactive 3D graphics software development system. Figure 1 shows the component structure of *Time-tunnel*. *Time-tunnel* consists of three main types of *boxes*, i.e., *data-wing*, *time-plane* and *time-bar*. *Boxes* mean software components provided by *IntelligentBox*.

(1) *Data-wing* has a shape like a sheet. In the first version of *Time-tunnel*, *data-wing* displays one multidimensional data, one time-series numerical data, as a chart on its sheet. For the visualization of multiple data, the user can use multiple data-wings as he/she wants. Each data-wing is connected to *time-bar* that works as its hinge. The hinge is also a *box* that has a rotation functionality called *RotationBox*. Therefore, through rotation operations on data-wings, the user can put multiple charts overlapped together to compare them.

(2) *Time-plane* also has a shape like a sheet. It is connected to *time-bar* vertically to *data-wings*. Usually, three *time-planes* are necessary as shown in Figure 2. Two *time-planes* are used to specify a time region, i.e., a begin time point and an end time point. As for the visualization of multidimensional data, these *time-planes* specify a certain set of attributes. As Figure 2 shows, correlation points between any two adjacent charts are displayed inside the time region. The remaining *time-plane* is used for displaying a radar chart.

(3) *Time-bar* has a thin, long cylindrical shape. *Time-bar* works as a time pivot of *data-wings*. It collects multiple time-series numerical data from each *data-wing* and displays a radar chart on one of the *time-planes*. It also displays correlation information between any two adjacent *data-wings* as scattered points in the time region specified by the two remaining *time-planes*.

Parent-child relationships among *data-wings*, *time-planes* and *time-bar* are defined as shown in Figure 1. *RotationBox* works as the hinge and the parent of *data-wing*, and *time-bar* is the parent of each *RotationBox*. *ExpandBox* becomes the parent of *time-plane*, and it works for positioning the *time-plane*.

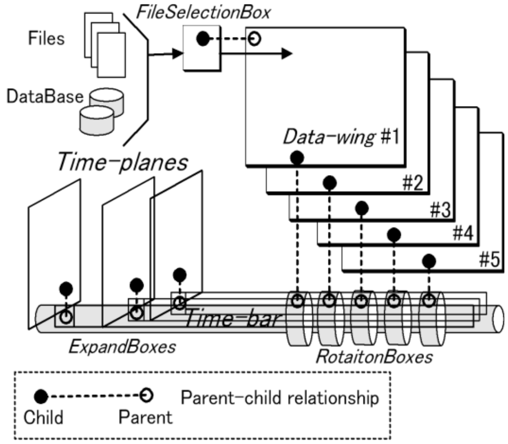


Figure 1. Component structure of *Time-tunnel*.

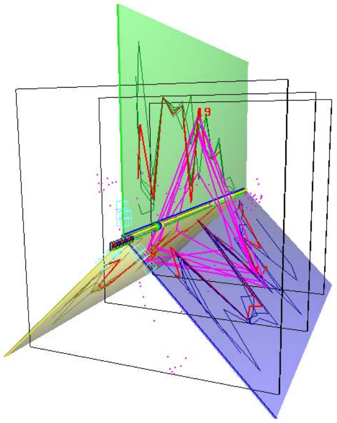


Figure 2. *PCTT* and its multiple radar charts.

B. Parallel Coordinates version of Time-tunnel(PCTT)

Although only one chart data is displayed on one *data-wing*, the visualization of multiple database records is possible by preparing exactly the same number of *data-wings*. However, when the user wants to visualize a huge number of data records, he/she has to prepare the same huge number of *data-wings* and practically it becomes impossible to manipulate them. To deal with this problem, as shown in Figure 2, we extended the functionality of *data-wing* to enable it to display more than one data records, i.e., multiple data records as multiple charts, in it like Parallel Coordinates. This is called Parallel Coordinates version of *Time-tunnel*(*PCTT*). With *PCTT*, even if there are a huge number of data record, the visualization for them is possible by dividing them into several groups and assigning each group to one of the multiple *data-wings* of the same *Time-tunnel*. Since the user can rotate and put any *data-wings* overlapped together, he/she can compare his/her selected records by looking at highlighted charts (red-colored charts) in Figure 2. Furthermore, multiple radar charts for the selected charts can also be displayed similarly to the original *Time-tunnel*. See Figure 2.

C. *Spline Parallel Coordinates*

Originally, *PCTT* displays multidimensional data records as multiple polylines. When the values of two adjacent axis (two attributes) of different data records are the same, the corresponding lines between the two axis are represented as only one line, and then this make it difficult to understand the number of such data records. To compensate this, we added spline mode that represents data records as splines instead of polylines as shown in Figure 3. This is very useful for visualizing network data (IP packets data) because the cases that port number and IP addresses are the same are frequently occurred.

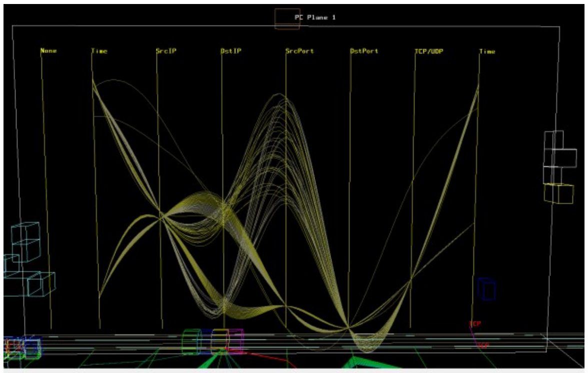


Figure 3. Spline Parallel Coordinates representation.

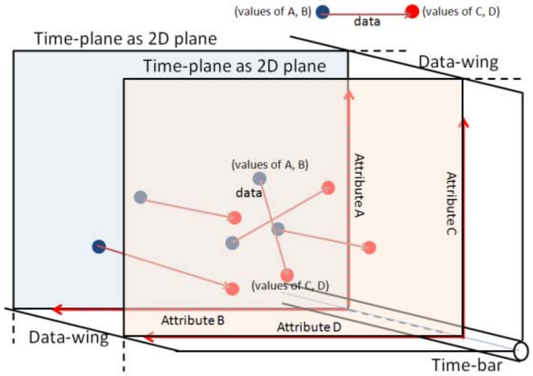


Figure 4. Conceptual image of *PCTT* with 2Dto2D visualization.

D. *2Dto2D visualization functionality*

For the network data visualization [4, 5], we also added 2Dto2D visualization functionality to *PCTT*. Its conceptual image is as shown in Figure 4. 2Dto2D visualization functionality displays multiple lines those represent four dimensional (four attributes) data drawn from one (2D of two attributes) plane to the other (2D of the other two attributes) plane. Using 2Dto2D visualization for multi-attribute data, it is easy to understand relationships about of the selected four attributes.

E. *Original 3D mode and new 3D mode functionality*

Another visualization example using *PCTT* is for learning analytics by visualizing learners' learning activity data [6]. The upper part of Figure 5 is one visualization example. At a glance, it is possible understand learning patterns of the whole learners. Conversely, it is difficult to understand each learning pattern. For visualizing it more clearly, we introduced 3D mode shown in the middle part of Figure 5 into *PCTT* as an aspect of 3D Parallel Coordinates. Actually, if adopting a 3D stereo display and stereo glasses like NVidia 3D Vison, it becomes easier to understand each learning pattern. However, 3D stereo system is expensive and its setting up is a bother. Therefore, we implemented more effective 3D mode shown in the lower part of Figure 5.

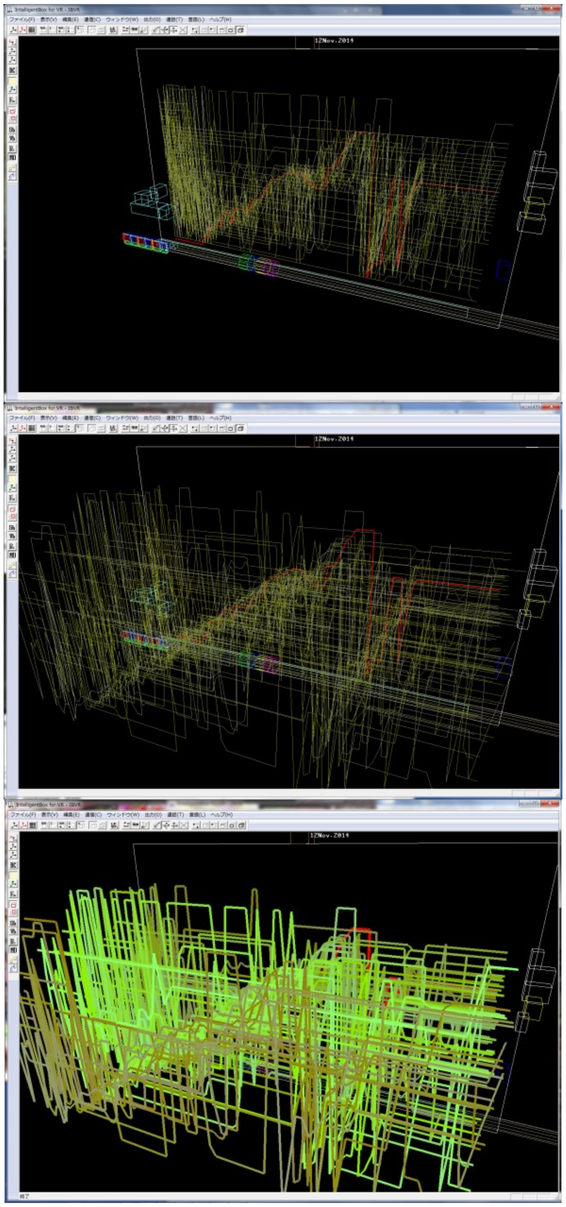


Figure 5. Original 3D mode and new 3D mode of *PCTT*.

In new 3D mode, the width of each line is changeable as specifying by the user and their colors are automatically changed gradually according to the order of data records. By setting the width value into thick, it becomes easier to distinguish each learner's learning pattern without 3D stereo system.

IV. NETWORK DATA VISUALIZATION USING *PCTT WITH 2DTO2D VISUALIZATION*

A. IP packet data

Network data is considered as a set of IP packets data. IP packet has several attributes, mainly source IP, destination IP, source Port, destination Port, Protocol type and Packet size. Using Parallel Coordinates, it is possible to represent each IP packet as one poly-line as shown in Figure 6. Individual axis corresponds to each of the attributes of IP packet data. Furthermore, Figure 7 shows 2Dto2D visualization image for IP packets. In this case, relationships between two attributes (source IP, source Port) to other two attributes (destination IP, destination Port) can be visualized. To detect intrusion attacks, this visualization is very significant because intrusion attacks have a certain access pattern strongly related to the four attributes of IP packet data.

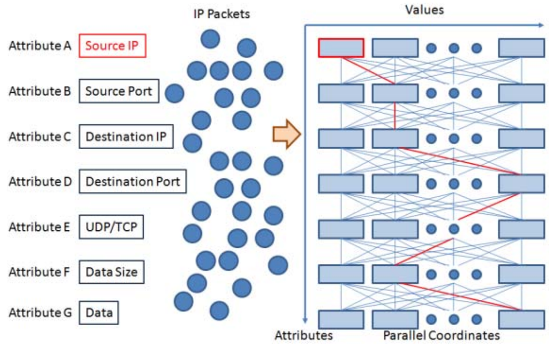


Figure 6. Parallel Coordinates visualization for IP packets.

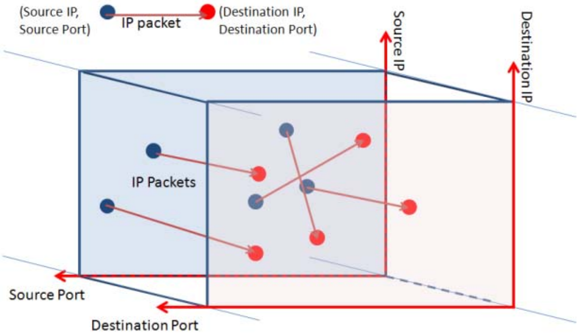


Figure 7. 2Dto2D visualization for IP packets.

B. PCTT with 2Dto2D visulization for IP packet data

Figure 8 to 11 show screen images of actual *PCTT* with 2Dto2D visualization for IP packet data. Here, we explain several components used for the visualization besides the main components of *Time-tunnel*. The several components of the left part in each figure are dedicated for setting a begin time and an interval time of captured IP packet data, and for displaying such data, e.g., the total number of IP packets in the day, the number of IP packets in the current interval time, etc. At the center location of each figure, 2Dto2D visualization is enabled. Since the four attributes set is the same as that of Figure 7, this case is suitable for the intrusion detection.

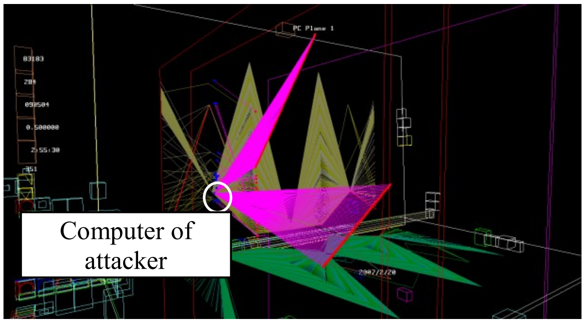


Figure 8. Access patterns of port scanning.

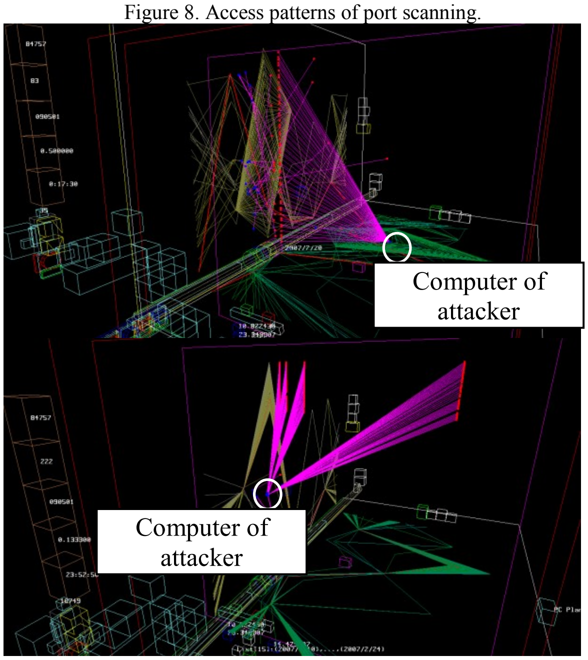
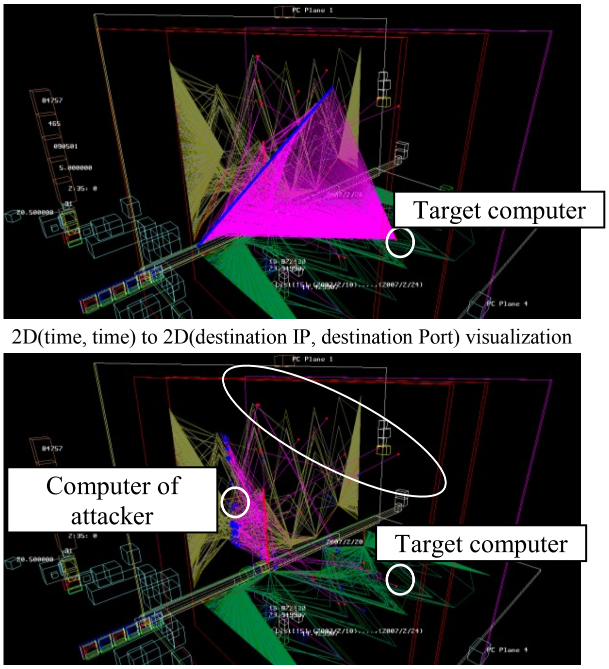


Figure 9. Access patterns of security holes attacks.

C. Intrusion detection

We use the darknet flow data of IP packets actually sent from the outside of our university and captured as pcap format files. Each file includes IP packets data in one hour and the average number of them in a file is roughly around 3,500. *PCTT* can read 24 hours files at once so that it can visualize IP packets data of one day at maximum. Also, we can specify an interval time and its begin time for visualizing IP packets data using the GUI of *PCTT* as previously explained. There is an automatic change mode for the begin time. In this mode, visualization results are automatically changed according to the begin time. When the interval time is 30 seconds, a begin time will be shifted every 30 seconds and one shift needs around 0.1 seconds as a real execution time. So, even if you want to check visualization results of IP packets in a whole day, you need only 5 minutes. This value is reasonable although it depends on the specification of the PC you use because we used a standard PC whose specification is as follows: CPU: Intel Core_i5, Memory: 4GB and no special graphics card.



2D(time, time) to 2D(destination IP, destination Port) visualization

2D(src IP, src Port) to 2D(dest IP, dest Port) visualization

Figure 10. Access patterns of DoS attacks

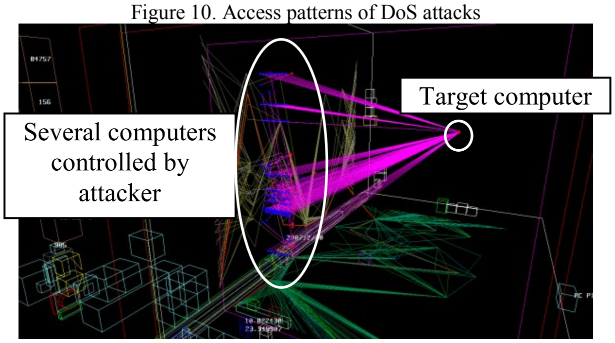


Figure 11. Access patterns of DDoS attacks.

The above figures seem a couple of network attack patterns those are actually detected using *PCTT* with 2Dto2D visualization, i.e., port scanning, security hole attacks, DoS(Denial of Service) attacks and DDoS(Distributed DoS) attacks, respectively. See [4, 5] for those details.

V. LEARNING ACTIVITY DATA VISUALIZATION USING *PCTT WITH 3D MODE*

A. Learning Activity data

Our Kyushu University employed e-Books viewer called BookLooper [16] produced by KYOCERA Communication Systems Co., Ltd, as one of the commercial cloud services in which users can read e-Books registered into the service through the Internet. This service gathers users' activity data of reading e-Books, for example, how long each user reads an e-Book, from and to which pages of the e-Book the user traverse. The attributes of such data are date, time, user name, material name that the user' access, and activity as a sequence of reading page indices. Since the fiscal year 2017, our university just started to employ BookRoll, another one of the e-Book viewers that has similar functionalities to BookLooper. Here, we adopt learning activity data of an information processing class collected by BookLooper from November 2014 to January 2015.

B. Visualization results of Learning Activity data

We applied *PCTT* for analyzing e-Learning activity data [6]. Fig. 12 shows two screen images as visualization results of *PCTT*. The upper figure of Fig. 12 is a bird eye view of the data for 12th, Nov. in 2014 in new 3D mode.

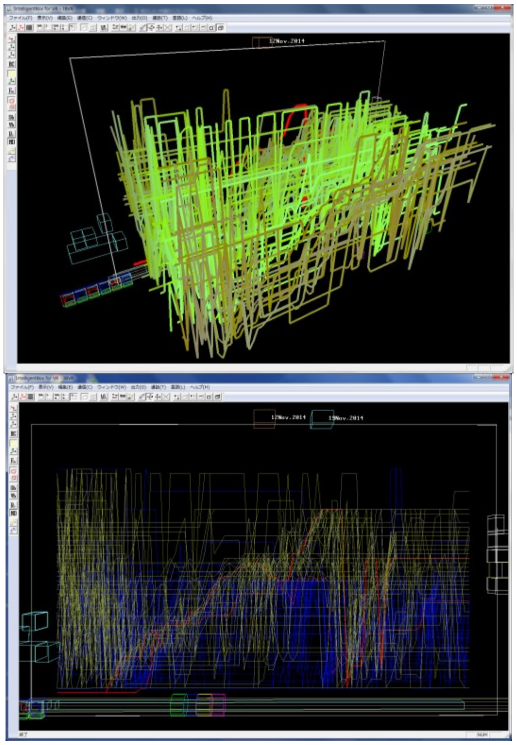


Figure 12. BookLooper data of 12th, Nov., 2014 in 3D mode(top) and BookLooper data of 12th and 19th, Nov., 2014 on two Data-wings overlapped together in 2D mode(bottom).

In this figure, each chart represents one student learning activity data and their total number is 80. The vertical axis means page numbers of an e-Learning material and the horizontal axis means the time. It is possible to highlight one of the charts as red color by specifying a student number. From this visualization result, it can be said that the most students took almost the same learning activity patterns like the red chart, which means the students looked at one page by one page sequentially maybe according to the teacher's talk. This pattern becomes unstable after the two-third of the total time. It may be because of a pause in the lecture at this time and the students started their exercises themselves. The other students who did not take this pattern may be the ones the teacher should pay his/her attention because some of the students stopped changing pages on the way.

Moreover, the lower figure of Fig. 12 shows the visualization of BookLooper data for 12th and 19th, Nov., 2014 on two Data-wings overlapped together in yellow color and blue color, respectively. From this visualization result, it is possible to understand the two learning activity pattern of the same students of 12th and 19th are very similar and the teaching patterns are also similar.

VI. Conclusions

In this paper, we treated a 3D visualization tool called *Time-tunnel*, especially described its aspects as 3D Parallel Coordinates by showing its actual visualization examples. Originally, *Time-tunnel* is a multidimensional data visualization tool and it was extended for Parallel Coordinates visualization called *PCTT*(Parallel Coordinates version of *Time-tunnel*). Furthermore, as its one aspect of 3D Parallel Coordinates, 2Dto2D visualization functionality was added. Although *PCTT* can visualize network data because IP packets consist of many attributes and such multiple attributes data can be visualized using Parallel Coordinates, 2Dto2D visualization functionality can more effectively visualize patterns of IP packets that seem network attacks. Although we have already proposed the combinatorial use of *PCTT* and 2Dto2D visualization functionality for the intrusion detection, this paper also introduced Spline Parallel Coordinates representation as one of the new features of *PCTT*. In addition, we proposed the use of *PCTT* for learning analytics by visualizing leaners' learning activity data and introduced 3D mode into *PCTT* to visualize each learner's learning pattern more efficiently. This 3D mode is regarded as 3D Parallel Coordinates. However, because such 3D mode was not enough to distinguish each learner's learning pattern, we implemented more effective 3D mode.

As future work, we are considering to employ some of the clustering methods and to introduce other 3D modes into *PCTT* for effectively visualizing data. Then, we will investigate more details about suspicious accesses of network data indicated as intrusion accesses using *PCTT* , and will investigate more various learners' leaning activity data for the learning analytics. Through these investigations, we will find out the problems of our proposed visualization tool and will improve it by solving the problems.

Acknowledgment

This work was partially supported by JSPS KAKENHI Grant Number JP16H02923.

References

[1] M. Akaishi and Y. Okada, Time-tunnel: Visual Analysis Tool for Time-series Numerical Data and Its Aspects as Multimedia Presentation Tool, Proc. of 8th Int. Conf. on Information Visualization (IV04), pp. 456-461,2004.

[2] A. Inselberg and B. Dimsdale, Parallel Coordinates: A Tool for Visualizing Multi-dimensional Geometry, Proc. IEEE Visualization 1990, pp. 361-378, 1990.

[3] H. Notsu, Y. Okada, M. Akaishi and K. Niijima, Time-tunnel: Visual Analysis Tool for Time-series Numerical Data and Its Extension toward Parallel Coordinates, Proc. of Int. Conf. on Computer Graphics, Imaging and Vision (CGIV05), pp. 167-172, 2005.

[4] Y. Okada: Network Data Visualization Using Parallel Coordinates Version of Time-tunnel with 2Dto2D Visualization for Intrusion Detection, Proc. of 27th Int. Conf. on Advanced Information Networking and Applications Workshops (WAINA), pp. 1088-1093, 2013.

[5] Okada Y. (2015) Parallel Coordinates Version of Time-Tunnel (PCTT) and Its Combinatorial Use for Macro to Micro Level Visual Analytics of Multidimensional Data. In: Xhafa F., Barolli L., Barolli A., Papajorgji P. (eds) Modeling and Processing for Next-Generation Big-Data Technologies. Modeling and Optimization in Science and Technologies, vol 4. Springer.

[6] S. Nakamura and Y. Okada: Learning Analytics Using BookLooper and Time-tunnel, Proc. of 11th International Technology, Education and Development Conference, pp. 8767-8776, 2017.

[7] Elena Fanea, Sheelagh Carpendale, and Tobias Isenberg, An Interactive 3D Integration of Parallel Coordinates and Star Glyphs. IEEE Information Visualization (InfoVis 2005), pp. 149-156, 2005.

[8] Nicter Cube of nicterWeb (http://www.nicter.jp/nw_public/scripts/cube.php)

[9] Keisuke Honda and Junji Nakano: 3 Dimensional Parallel Coordinates Plot and Its Use for Variable Section, Proc. in Computational Statistics, pp. 187-195, 2006.

[10] Yao Zhonghua, Wu Lingda: 3D-Parallel Coordinates: Visualization for time varying multidimensional data, 7th IEEE Int. Conf. on Software Engineering and Service Science (ICSESS), 2016.

[11] Troy Nunnally, Penyen Chi, Kulsoom Abdullah, A. Selcuk Uluagac, John A. Copeland and Raheem Beyah: P3D: A Parallel 3D Coordinate Visualization for Advanced Network Scans, IEEE Int. Conf. on Communications (ICC), pp. 2052-2057, 2013.

[12] Elke Achtert, Hans-Peter Kriegel, Erich Schubert, Arthur Zimek, Interactive Data Mining with 3D-Parallel-Coordinate-Trees, Proc. of ACM Int. Conf. on Management of Data (SIGMOD), pp.1009-1012, 2013.

[13] Jimmy Johansson, Camilla Forsell, Matthew Cooper: On the Usability of 3D Display in Parallel Coordinates: Evaluating the Efficiency of Identifying 2D Relationships, Journal of Information Visualization, 13(1), 29-41, January 1, 2014.

[14] Marc Streit, Rupert C. Ecker, Katja Osterreicher, Georg E. Steiner, Horst Bischof, Christine Bangert, Tamara Kopp and Radu Rogojanu; 3D Parallel Coordinate Systems – A New Data Visualization Method in the Context of Microscopy-Based Multicolor Tissue Cytometry, Int. Society for Analytical Cytology, Part A 69A: 601-611, 2006.

[15] Y. Okada, and Y. Tanaka, IntelligentBox: A Constructive Visual Software Development System for Interactive 3D Graphic Applications, Proc. Of Computer Animation '95, pp.114- 125, 1995.

[16] BookLooper, http://www.kccs.co.jp/ict/cloud-booklooper/ (on 15th, Dec. 2016).