2013 27th International Conference on Advanced Information Networking and Applications Workshops

Network Data Visualization Using Parallel Coordinates Version of *Time-tunnel* with 2Dto2D Visualization for Intrusion Detection

Yoshihiro Okada
Graduate School of Information Science and Electrical Engineering,
Kyushu University
Fukuoka, Japan
okada@inf.kyushu-u.ac.jp

***Abstract*—This paper treats network data visualization using Parallel Coordinates version of *Time-tunnel* (*PCTT*) for intrusion detection. Originally, *Time-tunnel* is a multidimensional data visualization tool and its Parallel Coordinates version provides the functionality of Parallel Coordinates visualization. It can be used for the visualization of network data because IP packet data have many attributes and such multiple attribute data can be visualized using Parallel Coordinates. In this paper, the authors propose the combinatorial use of *PCTT* and 2Dto2D visualization functionality for the intrusion detection. 2Dto2D visualization functionality, whose concept is originally derived from nicter Cube, 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 in a 3D space. This 2Dto2D visualization functionality was introduced to *PCTT*. Network attacks have a certain access pattern strongly related to the four attributes of IP packet 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, the authors show several network attack patterns visualized using *PCTT* with 2Dto2D visualization as examples for the intrusion detection.**

Keywords- 3D visualization, Parallel Coordinates, Time-tunnel, intrusion detection.

I. INTRODUCTION

This paper treats an interactive visual analysis tool for network data based on Parallel Coordinates version of *Time-tunnel* (*PCTT*) [1-2]. *Time-tunnel* [1] visualizes any number of multidimensional data records as individual charts in a virtual 3D space. Each chart is displayed on a rectangular plane and the user easily puts more than one different planes overlapped together to compare their data 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 multiple multidimensional data through interactive manipulations on a computer screen. However, in *Time-tunnel*, only one chart is displayed on one rectangular plane. So, if there are a huge number of data records, the user has to prepare accordingly such a huge number of rectangular planes and practically it becomes impossible to interactively manage them. To deal with this problem, we enhanced the functionality of *Time-tunnel* to enable it to display multiple chars like Parallel Coordinates [3] on each rectangular plane. This is called Parallel Coordinates version of *Time-tunnel* (*PCTT*) [2]. With this enhanced functionality, the user can visually analyze a huge number of multidimensional data records through interactive manipulations on a computer screen. The user can easily recognize the similarity or the difference among those data visually and interactively.

Parallel Coordinates version of *Time-tunnel* (*PCTT*) can be used for the visualization of network data because IP packet data have many attributes and such multiple attribute data can be visualized using Parallel Coordinates. Therefore, we also introduced 2Dto2D visualization functionality to *PCTT* for the intrusion detection of network data. 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 packet 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 as examples for the intrusion detection.

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 *Time-tunnel* and its Parallel Coordinates version with 2Dto2D visualization in Section 3. Then, Section 4 presents network data analysis examples. Finally we conclude the paper in Section 5.

II. RELATED WORK

Our Parallel Coordinates version of *Time-tunnel* (*PCTT*) can be used as the same visual analysis tool as Parallel Coordinates. Furthermore, *PCTT* visualizes multiple charts like Parallel Coordinates on one individual rectangular plane and it originally provides multiple rectangular planes in a virtual 3D space so that 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

978-0-7695-4952-1/13 $26.00 © 2013 IEEE
DOI 10.1109/WAINA.2013.185

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. As the similar tools, there are Star Glyphs of XmdvTool [5] and Stardinates Tool [6]. Stardinates Tool has combined feature of Parallel Coordinates and Glyphs [5]. There are also researches [7, 8] similar to this. Our *PCTT* has 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 [9-23]. The paper [10] proposes several interactive visualization methods for network and port scan detection based on PortVis[9], a tool for port-based detection of security events. Most of them are 2D and only volume visualization method uses 3D axes (Port high byte, Port low byte, and Time). The paper [11] proposes a visual querying system for network monitoring and anomaly detection using entropy based features. The paper [12] proposes ClockView for monitoring large IP spaces, which is a glyph in style of a clock to represent multiple attributes of time-series traffic data in a 2D time table. The paper [13] proposes the use of CLIQUE, a visualization tool of statistical models of expected network flow patterns for individual IP addresses or collections of IP addresses, and Traffic Circle, a standard circle plot tool. As Parallel Coordinates based visualization tools, there are VisFlowConnect [14] and trellis plots of Parallel Coordinates [15]. As treemap based visualization tools, there are NAVIGATOR [16], which displays detail information like IP addresses, ports, etc. inside each node of a treemap, and hierarchical visualization [17], which is a 2D map similar to a treemap in a 3D space. Also, there are visualization methods for network data using 3D plots [18] or lines in a 3D space [19-22]. DAEDALUS [22] is a 3D visual monitoring tool of the darknet data. However, there have not been any visualization tools like our *PCTT*. In this paper, we also propose 2Dto2D visualization functionality used with *PCTT*. The concept of 2Dto2D visualization functionality was derived from the visualization tool called nicter Cube [23], and there have not been any visualization tools like our *PCTT* with 2Dto2D visualization.

III. TIME-TUNNEL AND ITS PARALLEL COORDINATES VERSION WITH 2DTO2D VISUALIZATION

In this section, we describe the system configuration of *Time-tunnel* and its components and how *Time-tunnel* works for the analysis of multidimensional data, especially multiple time- series numerical data. Also, we introduce Parallel Coordinates version of *Time-tunnel*(*PCTT*) with 2Dto2D visualization. *Time-tunnel* is developed using *IntelligentBox* [4], which is a component-based visual and interactive software development system for 3D graphics applications.

A. System configuration of Time-tunnel

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*.

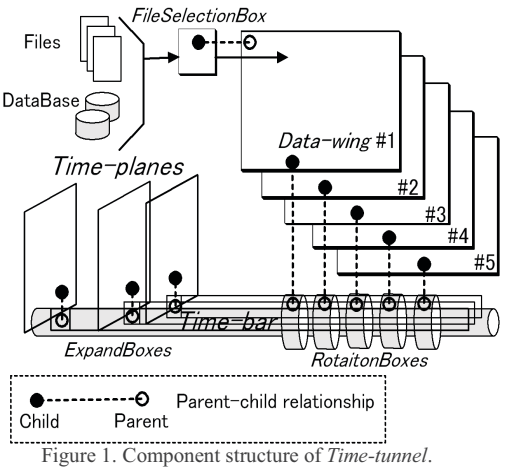


Figure 1. Component structure of *Time-tunnel*.

(1) Data-wing has a shape like a sheet. It 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 by its hinge. The hinge is also a *box* that has a rotation functionality called *RotationBox*. Therefore, by rotation operations on data-wings, the user can put multiple charts overlapped together to compare them. Each multidimensional data, time-series numerical data, of each data-wing is sent to time-bar through *RotationBox*.

(2) Time-plane also has a shape like a sheet. Time-plane is connected to time-bar vertically to data-wings. Usually, three time-planes are necessary as shown in Figure 1 and 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 shown in the upper figures of Figure 2, correlation points between any two adjacent charts are displayed inside the time region. The remaining time-plane is used for displaying a radar chart. Its position data is sent to time-bar to specify a time of data among charts to be displayed as a radar chart. Actually time-plane is connected to time-bar through *ExpandBox*. Time-plane moves along time-bar by the user manipulations on *ExpandBox* because *ExpandBox* is the parent of each time-plane.

(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.

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 3, 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 records to be visualized, 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* as show in Figure 3. 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. Furthermore, the radar chart for the selected charts can also be displayed similarly to original *Time-tunnel*.

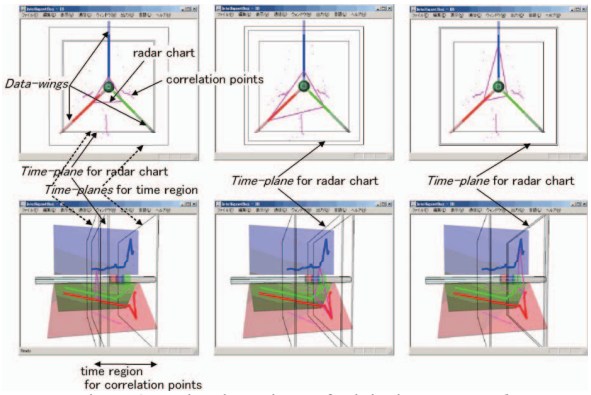


Figure 2. Radar chart views of original *Time-tunnel*.

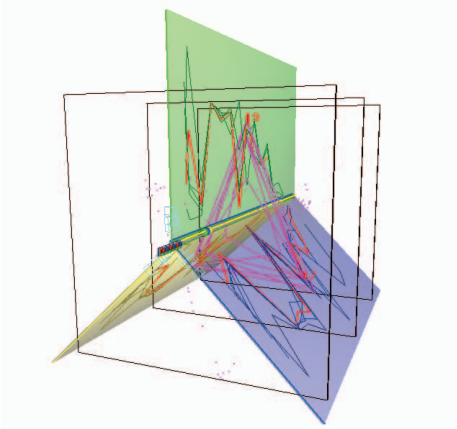


Figure 3. *PCTT* and its multiple radar charts.

C. 2Dto2D visualization functionality

For the network data visualization, 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 multiple attribute data, it is easy to understand relationships of the selected four attributes of each data. Figure 5 shows a screen snapshot of actual *PCTT* with 2Dto2D visualization. In this case, there are three data-wings so that there are three 2Dto2D visualization areas shown in the right figure of Figure 5.

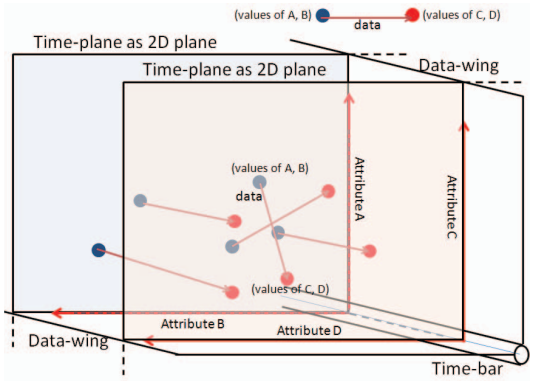


Figure 4. Conceptual image of *PCTT* with 2Dto2D visualization.

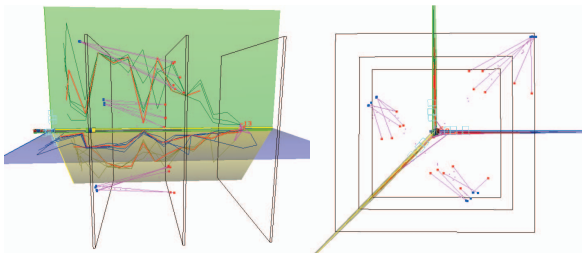


Figure 5. Screen image of *PCTT* with 2Dto2D visualization.

IV. Network Data Visualization using *PCTT* with 2Dto2D visualization

A. IP packet data

Network data is considered as a set of IP packet 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 among 2 attributes (source IP, source Port) to 2 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.

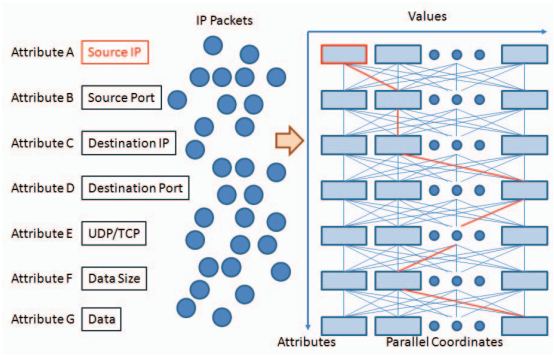


Figure 6. Parallel Coordinates visualization for IP packets.

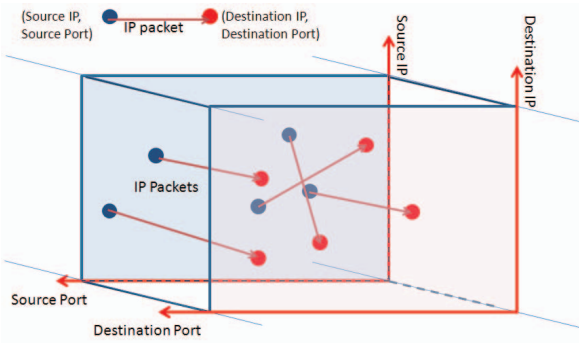


Figure 7. 2Dto2D visualization for IP packets.

B. PCTT with 2Dto2D viaulization for IP packet data

Figure 8 shows a screen image 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 top figure of Figure 8 shows the case that multiple radar charts and 2Dto2D visualization are both displayed. The several components of the left part in this 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. The middle figure of Figure 8 shows the case that only multiple radar charts are displayed. In this case, it is possible to easily understand the relationships between any two attributes of the four attributes each of which corresponds to each of the four data-wings about all IP packet data. Finally, the bottom figure of Figure 8 shows the case that only 2Dto2D visualization is enabled. Since the four attribute set is the same as that of Figure 7, this case is suitable for the intrusion detection.

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 packet 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 packet data of one day at maximum. Also, we can specify an interval time and its begin time for visualizing IP packet data using the GUI of *PCTT* as previously explained. There is an automatic change mode for the begin time.

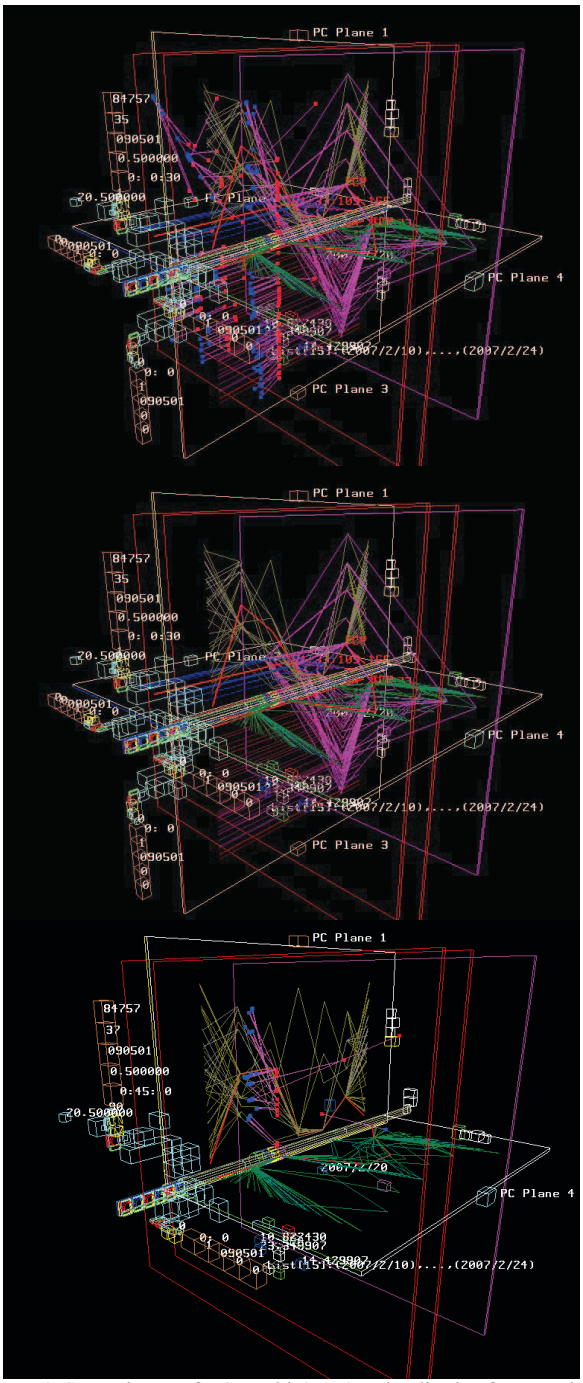


Figure 8. Screen image of *PCTT* with 2Dto2D visualization for IP packet data.

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 dependents 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. The followings are a couple of network attack patterns those are actually detected using *PCTT* with 2Dto2D visualization.

1) Port Scanning

Port Scanning is one of the most popular techniques attackers use to discover services that they can exploit to break into systems. During checking IP packet data of four days, we found only one case like port scanning as shown in Figure 9. In this case, a certain computer located outside of our university continuously access to computers of different destination IP and different but sequential destination Port of our darknet in a very short period.

2) Security Holes Attacks

Security holes mean shortcoming of a computer program (software code) that allows unauthorized users (attackers) to gain access to a system or network, and to interfere with its operations and data. Figure 10 is regarded to show access patterns of security holds attacks because they indicate the cases that the computer of an attacker tried to access many computers virtually located in our darknet by specifying certain destination ports.

3) DoS Attacks

DoS attack means Denial of Service attack. The most popular access pattern is one computer of an attacker simultaneously accesses many times to his/her target computer in a very short period. As a result, the target computer will become disenable to provide the services that the computer originally provided. Sometime, the computer will become malfunctioned. Figure 11 is regarded to show access patterns of DoS attacks because they indicate such a case. Indeed, the upper figure of Figure 11 shows different 2Dto2D visualization, i.e., 2D(time, time) to 2D(destination IP, destination Port). Therefore, blue points located from the left lower to the right upper mean the transition of the time about the corresponding IP packs those all tried to access to one target computer. As shown in the lower figure of Figure 11, their source IP and source Port are the same and then it can be found that the computer of an attacker is only one.

4) DDoS Attack

DDoS attack means Distributed Denial of Service attack. The most popular access pattern is more than one computers controlled by an attacker simultaneously accesses many times to his/her target computer in a very short period. As a result, the target computer will become disenable to provide its services. Sometime, the computer will become malfunctioned. Figure 12 is considered to show such access patterns.

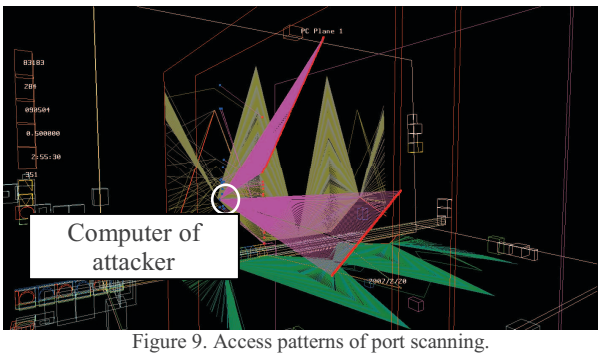


Figure 9. Access patterns of port scanning.

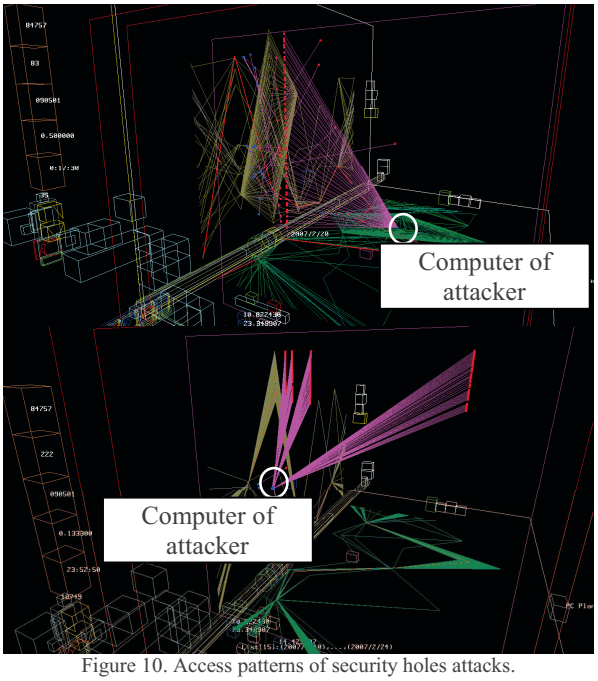


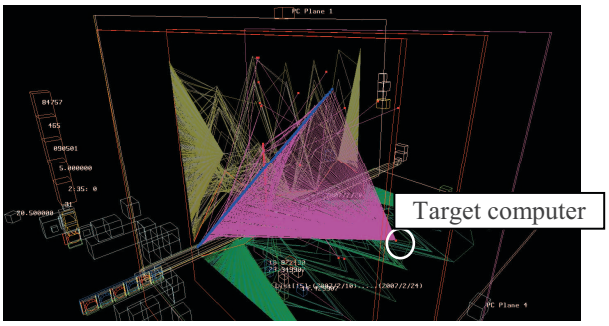
Figure 10. Access patterns of security holes attacks.

V. CONCLUSION

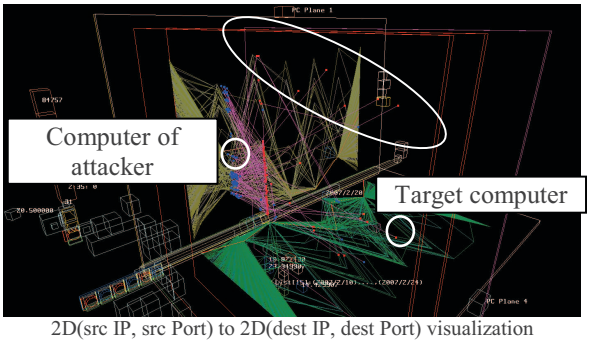
In this paper, we treated network data visualization using Parallel Coordinates version of *Time-tunnel* (PCTT) for the intrusion detection. Originally, *Time-tunnel* is a multidimensional data visualization tool and its Parallel Coordinates version provides the functionality of Parallel Coordinates visualization. It can be used for the visualization of network data because IP packet data have many attributes and such multiple attribute data can be visualized using Parallel Coordinates. In this paper, we mainly proposed the combinatorial use of *PCTT* and 2Dto2D visualization functionality. 2Dto2D visualization functionality displays multiple lines represented as relationships among four dimensional (four attributes) data drawn from one 2D (two attributes) plane to the other 2D (two attributes) plane in a 3D space. This 2Dto2D visualization functionality was added to *PCTT*. Network attacks have a certain access pattern strongly related to the four attributes of IP packet data, i.e., source IP, destination IP, source Port, and destination Port. So, 2Dto2D visualization is useful for detecting such access patterns. We shown several network

attack patterns actually visualized using *PCTT* with 2Dto2D visualization as examples of the intrusion detection.

As future work, we will investigate more details about suspicious accesses of network data indicated as intrusion accesses by the proposed visualization method. Also, we will try to investigate more various access patterns of the intrusion by visualizing statistic data of network flows of IP packets using the proposed visualization method.



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



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

Figure 11. Access patterns of DoS attacks

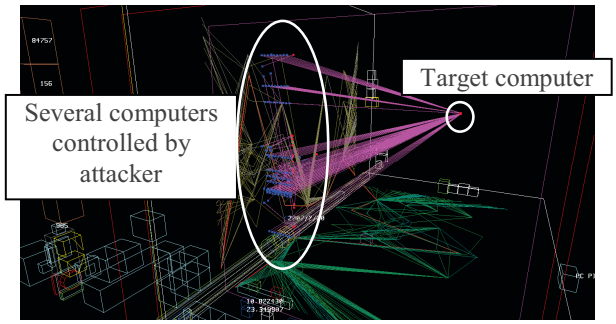


Figure 12. Access patterns of DDoS attacks.

ACKNOWLEDGMENT

This work was partially supported by Proactive Response Against Cyber-attacks Through International Collaborative Exchange (PRACTICE), Ministry of Internal Affairs and Communications, Japan.

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] 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.

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

[4] 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.

[5] http://davis.wpi.edu/~xmdv/news.html

[6] M. Lanzenberger and S. Miksch, The Stardinates - Visualizing Highly Structured Data, Proc. of Information Visualization IV'03, pp. 47-52, 2003.

[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] Christian Tominski, James Abello, and Heidrun Schumann, 3D Axes-Based Visualizations for Time Series Data, Poster Paper, IEEE Information Visualization 2005 (InfoVis 2005), 2005.

[9] J. McPherson, K.-L. Ma, P. Krystosk, T. Bartoletti, and M. Christensen. PortVis: A tool for port-based detection of security events, in ACM VizSEC 2004 Workshop, pp. 73-81, 2004.

[10] Muelder, C., Ma, K. L., Bartoletti, T., Interactive Visualization for Network and Port Scan Detection, A. Valdes and D. Zamboni (Eds.):RAID 2005, LNCS 3858, pp. 265-283, 2006.

[11] Alberto Boschetti, Chris Muelder, Luca Salgarelli, Kwan-Liu Ma, TVi: A Visual Querying System for Network Monitoring and Anomaly Detection, VizSec 2011 (The 8th Int. Symp. on Visualization for Cyber Security), Article No. 1.

[12] Christopher Kintzel, Johannes Fuchs, Florian Mansmann, Monitoring Large IP Spaces with ClockView, VizSec 2011 (The 8th Int. Symp. on Visualization for Cyber Security), Article No. 2.

[13] Daniel M. Best, Shawn Bohn, Douglas Love, Adam Wynne, William A. Pike, Real-Time Visualization of Network Behaviors for Situational Awareness, VizSec 2010, pp. 79-90, 2010.

[14] Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, Kiran Lakkaraju, VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness, in VizSEC/DMSEC'04, pp. 26-34, 2004.

[15] Stefan Axelsson, Visualization for Intrusion Detection – Hooking the Worm, Understanding Intrusion Detection Through Visualization Advances in Information Security Vol. 24, pp. 111-127, 2006.

[16] Matthew Chu, Kyle Ingols, Richard Lippmann, Seth Webster, Stephen Boyer, Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR, VizSec 2010 (The 7th Int. Symp. On Visualization for Cyber Security), pp. 22-33, 2010.

[17] Takayuki Itoh, Hiroaki Takakura, Atsushi Sawada and Koji Koyamada, Hierarchical Visualization of Network Intrusion Detection Data, IEEE Computer Graphics and Applications, pp. 40-47, March/April 2006.

[18] Stephen Lau, The Spinning Cube of Potential Doom, Communications of the ACM, pp. 25-26, June 2004/Vol. 47, No. 6.

[19] Weichao Wang, Aidong Lu, Visualization Assisted Detection of Sybli Attacks in Wireless Networks, VizSEC'06, pp. 51-60, 2006.

[20] Erwan Le Malecot, Masayoshi Kohara, Yoshiaki Hori, Kouichi Sakurai, Interactively Combining 2D and 3D Visualization for Network Traffic Monitoring, VizSEC'06, pp. 123-127, 2006.

[21] Jon Oberheide, Manish Karir, Dionysus Blazakis, VAST: Visualizing Autonomous System Topology, VizSec'06, pp. 71-79, 2006.

[22] Inoue, D., Suzuki, M., Eto, M., Yoshioka, K. and Nakao, K., DAEDALUS: Novel Application of Large-Scale Darknet Monitoring for Practical Protection of Live Networks, E. Kirda, S., Jaha, and D. Balzarotti (Eds.): RAID 2009, LNCS 5758, pp. 381-382, 2009.

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