2009 Third UKSim European Symposium on Computer Modeling and Simulation

Study On Advanced Visualization Tools In Network Monitoring Platform

Doris Wong Hooi Ten, Selvakumar Manickam, Sureswaran Ramadass & Hussein A. Al Bazar

National Advanced IPv6 Centre (NAv6)
Universiti Sains Malaysia
Penang, Malaysia
{doris, selva, sures, hussein}@nav6.org

***Abstract*— Visualization tools have emerged as a critical component, especially in medical, education, engineering, military and environmental management. These fields have applied the visualization techniques to improve decision making and organization management performance. In recent times, with the advent of Internet and the explosive growth of networking infrastructure on a global scale demand for an intuitive and wholesome approach to visual the network traffic. Complexity of network architecture and insufficient vendor support are the major issues always that are faced by a user in solving a network monitoring problem. Network engineer needs to start on network monitoring by integrating conventional network monitoring tools with an innovative visualization tool, which can provide the network activities that are easily understood by a user. Currently, there are numerous data visualization tools in network monitoring namely Network Analysis Visualization, Spinning Cube of Potential Doom (SCPD), Visual Information Security Utility for Administration Live (VISUAL), SeeNet, Cichlid, CyberNet and others. These tools provided useful information about network activities, which important for monitoring purpose. Our work entails the development of an advanced visualization framework to intelligently visualize high volume, real-time network traffic data.**

Keywords- data visualization, network traffic visualization, network monitoring

I. INTRODUCTION

Many organizations depend on network monitoring for making decisions and judgment on large volumes of dynamic network data. Networks can be monitored based on methods such as statistical intrusion and abnormal detection for attacks or malicious. The old saying that “a picture is worth a thousand words” often understates the case, especially with regard to moving images, as our eyes are highly effected by evolution to interpreting a movement and detecting the changes of surrounding. Therefore, network monitoring is an important demanding task. The task is even more complicated when dealing and working with highly dynamic information. However, reduction of the complicated network traffic data into simple information and visualize it into a suitable platform are significant challenges for a network administrator.

There are many visualization tools that strive to present data for the network administrator. The result from the monitoring can be being presented in multi-variate, multi-level 2D and 3D representation. There were many types of visualization tools for network monitoring. However, not all data representations provide sufficient, relevant information for the network administrator. In order to provide robust decision support quality information to allow the administrator seamlessly monitor the network, data must be analyzed and relevant and salient features must be extracted and presented.

Advanced visualization approaches present data in an intuitive and understandable manner and it is more comprehensible to the network administrator. The purpose of this paper is to review the existing data visualization tools in network monitoring in order to reveal the problems from the network an overview of network monitoring problems. Based on the review of the tools, we propose a suitable visualization methodology of network scans can serve as an interpretive platform and enhance human insight.

This paper is organized as follows. In section II of this paper, we present an overview of the network monitoring problems. Follow by presenting and discussing the existing data visualization tools in network monitoring in section III. In section IV, we proposed a visualization methodology for network monitoring following by a conclusion of the paper.

II. OVERVIEW OF NETWORK MONITORING PROBLEMS

Monitoring is an important component for providing a reliable service and pre-tempting any potential downtime or issues. The necessary part on the services is the requirement to monitor and analyze the network traffic flowing through the system. In order to identify the problem, there are two types of monitoring, namely, real time monitoring and historical data collection/analysis.

Real time monitoring involves incorporation of trouble ticket and alerting system. Ideally, the monitoring tool can tell users when a network routing problem and unusual condition occurs (e.g. mis-configured devices, virus or worm attack, and application faults) [1]. Historical data collection and analysis involve two activities, data collection and data viewing. Data collection includes the

978-0-7695-3886-0/09 $26.00 © 2009 IEEE
DOI 10.1109/EMS.2009.24

recording of long term uptime, usage and performance statistics in order to graph and analyze the data [1].

Both monitoring forms are able to use standard protocols such as Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP). SNMP is designed to monitor/record the performance of network protocol and devices (e.g. router, hub, server, printer or modem) [1]. Any failure detected in the network, such as router and host outages or buffer overflow, must be identified and located before the network engineer can respond accordingly.

Network complexity also is an issue when it comes to monitoring. Identifying and locating faults naturally becomes more difficult with large and more diverse networks. This issue can be addressed by visualization. Using a network monitoring system integrated with innovative visualization tools can vastly improve the network administrator's response time and can speed up the troubleshooting. This also brings up the more pressing issue of scalability. Scaling to a large network topology with high data rates require a larger number of monitoring devices with great processing power. The ability to actually collect data in real time (or with low latency) and the extent of data collection required depends immensely on the capacity of the monitoring appliance to be used. Data collection can be as simple as Up/Down monitoring but can go as far as performance monitoring, net flow (to check the traffic flow), or even data capture (to analyze each packet). For more intensive usage such as data capture, the monitoring device has to be powerful enough to handle high load and big traffic streams.

Likewise, vendor support becomes one of the network monitoring issues [2]. Issues arising due to the complexity of network architecture cannot be interpreted easily and makes it difficult to get support from vendors when we have a network problem. When an outage in an overly complicated network occurred, network engineer will try to discover the problem or via discussion with local user or vendor. With current visualization technology, vendor support might not be useful for identification of a network problem because they could face the difficulty to understand the complicated network architecture by using convention visualization tools (2D and 3D visualization) [2].

With this regards, network engineer will waste a lot of time trying to understand the configuration before coming up with a suggestion to fix the problem. The time taken to do this will inadvertently affect the productivity of the particular organization, leading to loss of profit. In order to counter this problem, system developers need to replace the convention network monitoring system with a confluence of a network management system and innovative visualization tools, which will show the network activities in a virtual environment. When used with visualization support, network uptimes and consistency can be significantly improved.

III. Existing Data Visualization Tools In Network Monitoring

There are number of tools in the visualization area that have applied on the network monitoring. Commonly, network security monitoring is the part that most of the visualization applications have focused on more compared with others. Information on malicious attacks that have been triggered on an abnormal detection device will be presented to the network administrator [3]. There are some other areas that visualization tools have focused on such as telephone networks and network management.

The major problem for network traffic analysis remains to the constantly increasing volume of network traffic and the inability of conventional network monitoring tools that can provide a good overview of traffic patterns [3]. It is difficult to gain the understanding of nature of the network traffic data by using conventional interface when standard network sniffers are used on large data sets, the output quickly becomes unmanageable. Likewise, home and enterprise users also demand a high security cyberspace where they can do their online business without any intrusions. So, they are becoming more interested in network traffic analysis but the existing network scanning tools with conventional visualization tools do not meet their requirements.

Visualization techniques such as 3D Scatterplot, line graph, survey plot and bar chart are some examples from Network Analysis Visualization (NAV) that provide overview and detail IP address and services, which are retrieved from a network monitoring system [3]. NAV shows the network data in different textual and selected colors which based on the different services, ports and IP address as well as the capability to aggregate and remove connections among other features [3]. Moreover, some key aspects of this problem have been addressed with the NAV solution, and visualization approach complement statistical detection methods is sufficiently extensible to provide a wider range of capabilities. However, the problem with this model is transferring the large network monitoring data from a computer network system into a reliability virtual environment. Likewise, whether it can provide sufficient information or not to help a beginner to monitor and make a decision regarding the anomaly that has occurred in their network system.

Other network security visualizations such as Spinning Cube of Potential Doom (SCPD) is designed for network professional and also presented simple information on the network security frequency and threats extent to beginner [4]. An example of SCPD has been shown in Figure 1. A complete map of internet address space indicating the frequency and origin of scanning activity will be provided by SCPD. User can be able to visualize easily about the sensor data from a large network. Rainbow color map has been used for the cube colors dots of incomplete connections [3]. Port scans on a single host represented by vertical lines and others scan across hosts will be represented by horizontal lines.

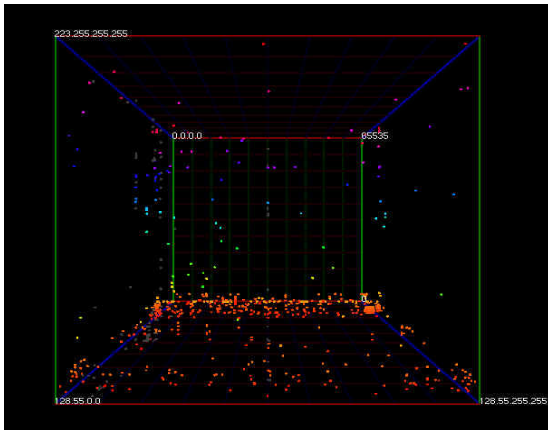
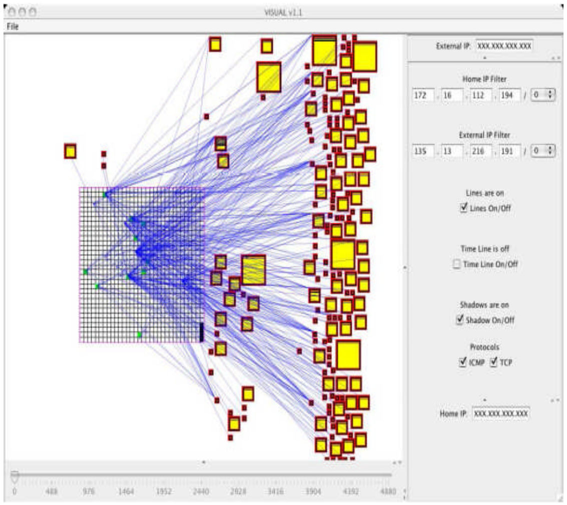


Figure 1. Network Security Tool - Spinning Cube of Potential Doom.

Another network security visualization tool is Visual Information Security Utility for Administration Live (VISUAL). VISUAL is a tool that allows network administrators to examine the communication networks between internal and external hosts, in order to rapidly aware the security conditions of their network [5]. VISUAL applied the concept of dividing network space into a local network address space and a remote network address space (rest of the internet). In order to produce its data visualizations, data will be taken from the log files of TCP-Dump or Ethereal [6][7]. The advantage of VISUAL is to provide a quick overview of the current and recent communication patterns in the monitored network. Administrators can specify their network and remote IP by using home and remote IP filter as shown in Figure 2. Based on the information provided by IP filter, administrators can identify any single external hosts that are connected with the number of internal hosts from a grid, which may be relevant to be used in their network. The grid represents home hosts; based on connection lines it allows the network administrator to check the total traffic that exchanged between home host and external host [5].



External IP: XXX.XXX.XXX.XXX

Home IP Filter
172 . 16 . 112 . 194 / 0

External IP Filter
135 . 13 . 216 . 191 / 0

Lines are on
☑ Lines On/Off

Time Line is off
☐ Time Line On/Off

Shadows are on
☑ Shadow On/Off

Protocols
☑ ICMP ☑ TCP

Home IP: XXX.XXX.XXX.XXX

Figure 2. VISUAL is a tool that allows user to check communication network between internal and external hosts.

Data is dumped to a file or piped through a file stream without an organization to the semantics of the data. Due to lack of discarded of the query interface in the traditional network monitoring system, network administrators have to be responsible for managing and defining the huge and complicated data.

New approach was taken by Gigascope. It has applied a SQL interface to the network monitoring system, greatly simplifying the task of administering and interpreting a flow of data. The clear semantics of the data streams allow this tool to perform aggressive optimizations, such as completing most or all of a query on the Network Interface Card (NIC) [8].

There were some of the tools that used to study about the 2D and 3D representations such as SeeNet and SeeNet3D [9][10]. Helix-based graph layout and geographical representations are the techniques' examples [3]. Based on these tools, telephone network can be monitored for detecting an anomaly [11]. Techniques such as zooming, panning, rotation described in [12] can be used to interact with the representations.

Cichlid is a client and server visualization tool which is designed with remote data generation and machine independence in order to allow the user to view real time network data in 3D visualization. The displayed data is transmitted from servers to the client engine [13]. It presents high-quality 3D, animated visualizations of a wide range of network analysis related data sets for the user [13].

CyberNet is a project to present network management in automatically build virtual environment. Figure 3 shows the CyberNet framework. It is implemented by using Java, Visual Reality Machine Language (VRML) and CORBA [14].

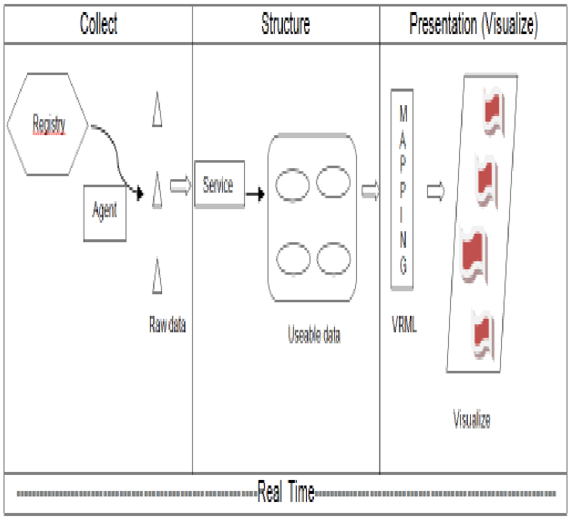


Figure 3. CyberNet framework.

This technique can visualize the network status in a virtual reality environment and will be more comprehensive to a wider range of users. The rapid understanding of the network data helps novice network administrators in monitoring dynamic network data. The data collecting layer is responsible for collecting raw data from a registry system which dispersed throughout the network. A Collector is designed to collect the necessary data that required by the particular services/parameter automatically according to the predefined policies. Afterward, collector will transfer all the raw data that had been collected to the second part of the framework namely data structuring layer. The data structuring layer is responsible for accepting the data from the data collecting layer and rearranges the data into a useable form which will be dumped again into a number of files accordingly. The final part of this framework will be the network monitoring data presenting part. The arranged data files will be transferring into the data presenting layer for displaying in the virtual environment. The user can interact in several ways with the system. Mechanisms for data clustering are provided, as well as mechanisms for visualizing data with different levels of detail, dependent on the distance between the user and the data being observed [15].

IV. Proposed Visualization Methodology For Network Monitoring

In this paper, we proposed a visualization methodology for network monitoring. Generally, visualization tends to be an iteration process. Basically, our proposed methodology will be an enhancement of the existing CyberNet visualization tools. The enhancement revolves around the collection, structuring as well as presentation modules on visualization methodologies. There will be two agents in data collection section to solve the data searching overhead problem. Data mining technique such as association rules will be applied in data structuring section to verify the usefulness of the tool. Data mapping will be the important issue to be discussed in the paper. The proposed visualization methodology and framework will be shown in Figure 4 and Figure 5.

A. Data Collection

Instead of one agent responsible in collecting, structuring and transferring, there will be two new basic agents that we proposed in this section. Agent *seeker* will seek and collect for certain data that requested by particular network administrator and store in a database. Another proposed agent named *transferor* in this layer will continue to structure and transfer the data. Data from the database will be transferred to data structuring section for further process. Overhead in this system will be avoided.

B. Data Structuring

Data mining is a powerful technology to help in data structuring section. Technology in extracting of hidden predictive information from the large database will be applied. Based on different categories' criteria, data will be restructured, rearranged and located into pages. Agent *scanner* will work active in scan the full pages and form them into useable relation tree structure view. This is to address any breakdown in the system. Update of data can be done continuously. Association rules will be concerned in this section in order to produce a comprehensive relationship between tree structure and data. Agent named *receptionist R1* working in recording and keeping track pages configuration and *receptionist R2* will take responsibility to ensure the consistency and efficiency on every single update data to be structured to the relation tree structure.

C. Data Presentation

Different visualization and environment modules (e.g. hypercube technologies, 3D sound, virtual reality, internal network space) will be provided in this section for the network administrator to choose. An agent named *carrier* will be shown in this section. *Carrier* takes responsible in bringing the selected module from the network administrator to mapping process before displaying the intuitive data to the network administrator. Network administrator is allowed to choose and tweak the visualization (haptic input) and for details viewing and navigation. Multimedia elements (e.g. animation, video, text) will be included in this section. The integration between comprehensive data and multimedia elements will be presented to the network administrator.

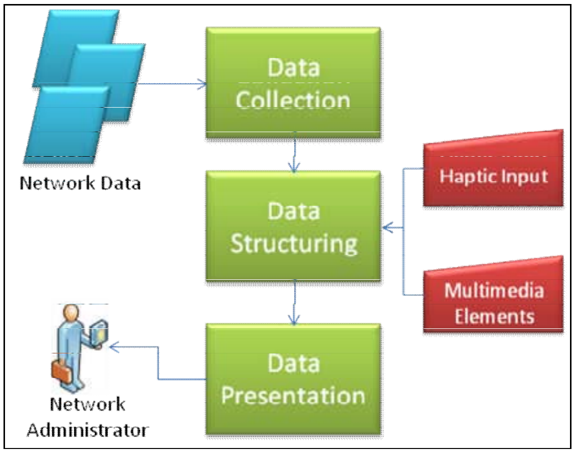


Figure 4. Proposed Visualization Methodology.

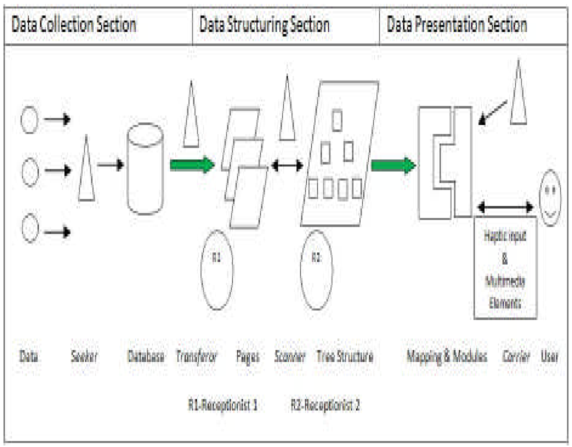


Figure 5. Proposed Visualization Framework.

V. CONCLUSION

This paper provided an overview of network monitoring problems, and reviewed various existing data visualization tools such as Network Analysis Visualization, The Spinning Cube of Potential Doom, VISUAL, SeeNet3D, SeeNet and CybetNet have been discussed in the paper. However, we believe our proposed visualization methodology for network monitoring will be able to simplify the presentation of a complicated network monitoring data into a more systematic and comprehensive interpretation platform.

ACKNOWLEDGMENT

Special thanks to colleagues of the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia for their willingness to spare their time, guidance, sharing their knowledge and support. This paper will be a part of the new research in NAv6.

REFERENCES

[1] N. F. Mir, Computer and Communication Networks, Prentice Hall, 2006.

[2] T. A. Limoncelli, C. J. Hogan, S. R. Chalup, The Practice of System and Network Administration, 2nd Edition, Addison-Wesley, 2007.

[3] M. Allen, P. McLachlan, “NAV Network Analysis Visualization,” University of British Columbia, [Online, 29 May 2009].

[4] S. Lau, “The Spinning of Potential Doom,” Commun. ACM, 47(6):25–26, 2004.

[5] R. Ball, G. A. Fink, and C. North, “Home-centric visualization of network traffic for security administration,” VizSEC/DMSEC ’04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 55–64. ACM Press, 2004.

[6] V. Jacobson, C. Leres, and S. McCanne, TCPdump public repository, http://kb.pert.geant.net/PERTKB/TcpDump, cited September, 2009.

[7] G. Combs. Ethereal downloadable at: http://www.ethereal.com/,cited September, 2009.

[8] C. Cranor, Y. Gao, T. Johnson, V. Shkapenyuk, O. Spatcheck, “Gigascope: High Performance Network Monitoring with an SQL Interface,” SIGMOD’ 02, ACM, 2002.

[9] R. A. Becker, S. G. Eick, and A. R. Wilks, “Visualizing network data,” IEEE Transactions on Visualization and Computer Graphics, vol. 1, no. 1, pp. 16–28, 1995.

[10] K. C. Cox, S. G. Eick, and T. He, “3D geographic network displays,” SIGMOD Record, vol. 25, no. 4, pp. 50-54, 1996.

[11] K. C. Cox, S. G. Eick, G. J. Wills, and R. J. Brachman, “Visual data mining: Recognizing telephone calling fraud,” Data Mining and Knowledge Discover, vol. 1, no. 2, pp. 225-231, 1997.

[12] T. He and S. G. Eick, “Constructing interactive network visual interfaces,” Bell Labs technical Journal, vol. 3, no. 2,pp. 47-57, Apr. 1998.

[13] J. A. Brown, A. J. McGregor, and H-W Braun, “Network performance visualization: Insight through animation,” Proceedings of the Passive and Active Measurement Workshop, 2002.

[14] D. S. C. Russo, P. Gros, P. Abel, D. Loisel, J-P Paris, “Using Virtual Reality for Network Management: Automated Construction of Dynamic 3D Metaphoric Worlds,” 1999.

[15] R. J. Hendley, N. S. Drew, A. M. Wood, and R. Beale, “Narcissus: Visualising information,” Proc. IEEE Symp. Information Visualisation, 90-96, Oct. 95.