Detecting Networks Anomalies and Attacks Using 3D Visualization

Besnik Camaj*, Etienne Petremand

Department of Software Engineering, University of Applied Sciences of Western Switzerland, Switzerland

Copyright © 2015 Horizon Research Publishing. All rights reserved.

Abstract 3D modeling and visualization has become a key component of scientific research and development in many domains. Adding new routers, switches or firewalls, the computer networks are becoming more and more complex. The paradigm of introducing computer networks in three dimensions helps a lot to protect and provide services to networks. Therefore, the main purpose of this paper is detecting the network anomalies based on a 3D visualization of computer network. The interactivity between network administrator and the application happens in real-time. This means that if a breakdown occurs, the network administrator will be informed in real time and will be able immediately to switch off the broken device and then repair it. Practically, we realized a 3D modeling and visualization of our university computer network with more than thousand devices and it works well.

Keywords 3D Modeling, Visualization, Computer Network, Interactive, Network Attack, Real Time

Visualization for network security has become an interesting research topic. With the progress of technology and the implementation of new requirements, computer networks are more complex and very often attacked. Presenting the computer network in three dimensions helps manage these alerts. « There are many potential applications of information visualization to the problems of computer security, including: Visualization for detecting anomalous activity, Visualization for discovering trends and patterns, visualization for correlating intrusion detection events, visualization for seeing worm propagation or botnet activity, visualization for forensic analysis, visualization for understanding the makeup of malware or viruses, visualization for communicating the operation of security algorithms etc. » [1].

Here we will describe the 3D-NET, a practical application that deals with 3D modeling and visualization of our university computer network. Usually we had the different schemas, tables and we print them to use for further needs. If we had to change a network device, previously the network administrator looked at the identification of that device in a plan and then he had to check another plan for the location. This could be quite easy if the network has a few devices (Figure 1).

1. Introduction

Figure 1. A computer network in 2D with only 12 devices

2. Methods and Technology Used

2.1. The Problem

How to present a computer network that contains more than a thousand devices connected to each other through various link weights and how to maintain it in a real-time? Presenting the computer networks in 2D, with traditional visualization techniques on a paper or on a display, are extremely inconvenient. The network administrator is not able to have a clear view if a trouble occurred in network. In this context, the problems arose all of the time, especially with the cyber attacks.

2.2. Solution

Faced with the problem described above, our idea was to find a convenient form in order to visualize and control a computer network in real-time. In our institute, we realize different applications in 3D modeling and visualization technology. So the idea to find a solution of this problem was based on three-dimensional representation of computer network. In the beginning, we started with a prototype - modeling a network of only few devices (Figure 2).

Figure 2. A simple network in 3D

The links between devices are represented with different color segments for different weights. Once given the number of network components, the possibility of choosing the network modeling was a good advantage. In our application, we took the different network devices like servers, routers, switches, firewalls, giving each other their standard form. The third dimension - the depth, makes the appearance of the network more naturally. The relevant form of parallelepiped was used to represent servers, hubs and other nodes like switches. The cylinder represents a router and finally a

computer screen represents the computers on the network. Each network device is identified with IP address (Figure 3).

Figure 3. Zooming 3D-NET

For a node group, we choose a 3D conical shape where the top of the cone represents a router and in its circular base are placed the computers. After a test we made, this application run well. Then we completed the network structure of our university, which contains over a thousand network devices. Using the mouse, it is easy to navigate and visualize the entire network within a screen. To quickly distinguish the link weights of the network, the color as a key tool in visualization is used (Figure 2). For better visualization of nodes and network devices and specially to minimize a crossed links, the distance between nodes related to the weight of the link, is given by:

$$d_{ij} = 1 / w_{ij} \quad (1)$$

d_{ij} = displayed link length, w_{ij} = weight of the link

That means the distance between two nodes is inversely proportional to the link weight [5].

2.3. Technology Used

For modeling and visualizing the network, the programming language C++ is used with a graphical library Open Scene Graph. Open Scene Graph is an open source high performance 3D graphics toolkit, used by application developers in fields such as visual simulation, games, virtual reality, scientific visualization and modeling [2]&[14].

The network structure is identified through XML files, where each node has its parameters (name, type, state and IP address, (Figure 4).

id	name	type	state	address_ip
1	Internet	Internet	enable	
2	Default gateway	router	enable	
3	switch01	switch	enable	
4	switch02	switch	enable	
5	hub01	hub	enable	
6	tcdc01	server	enable	10.192.72.56
7	tcdc02	server	enable	10.192.72.57
8	EDU-PC101	pc	enable	10.192.73.106
9	EDU-PC102	pc	enable	10.192.73.107
10	EDU-PC201	pc	enable	10.192.73.206
11	EDU-PC202	pc	enable	10.192.73.207

Figure 4. An XML file, describing the structure of a network node

As a dynamic support of network visualization, we added a real-time interactivity between network administrator and application. If a problem occurs in a network, the alert messages are instantly generated from the security devices through log files. At the same time we made possible the identification of risked zone, the white sphere (Figure 5).

Immediately, the white sphere with the origin on that device will be drawn to attract the administrator eyes. At the same time an emergent sound will be played. The network administrator will be informed in real time (through SMS as well if absent in a working place). We can zoom and the alerted device will be shown on the screen with the red color with all necessary information written on it (Figure 6). This is based from information visualization mantra (Ben Shneiderman) [4]: Overview first, zooming and filter, then details on demand ».

Figure 5. Detected overloaded network area (White sphere)

(A)

(B)

Figure 6. The network administrator informed in real time via SMS (A) or via controlling display (B)

Consulting its identification and the location of a problematic device, the administrator can first switch that device off and then go directly in a location where it is based to repair it (or even to change it completely). This kind of network visualization allows even untrained users to detect and repair these devices. As Ball, Fink and North said « Regardless of training or experience, administrators must be able to rapidly understand the security state of their systems and networks, especially during a crisis. Most of the tools they use are text-based. We believe they can be more effective using visualization » [3].

2.4. Future Work

Many researchers in the physical sciences have utilized 3D data visualization techniques to explore the interaction of variables that simultaneously impact physical phenomena [11]. We can incorporate network traffic data into the display, letting administrators quickly examine the data for particular types of traffic, such as illegal systems on the network, improper application usage, or connections from unknown systems or users. [12].

It is interesting to visualize the flow of communication across the network. For the network link weights, we can use the spectral order of colors to indicate different values, from the lowest to the highest one. Several applications have been

developed to promote research in the area of visualization for network security. There are several applications that visualize the network traffic data [6]. As an example, the VISUAL 3D scene is made of two network pixel maps facing each other as if in a mirror. A network pixel map is a pixel-oriented overview visualization [7]. One another application enables users to dynamically construct multiple-view visualizations for their tasks and data. Users exploit powerful visualization components developed in research such as Hyperbolic trees and Treemaps [9]. This may be useful because proficient hackers will attempt to hide their ultimate goal [10]. Further more, from the Tellenbach study, it is seemed that each routers shows different visibility of the anomalies. That difference illustrates the impact of the traffic mix on the anomaly visibility [15]. In this sense, in our application we can still add different data analysis in order to answer different requirements.

3. Conclusions

In this paper, we described the 3D-NET, an application that facilitates the maintenance during the network problems (malicious attacks, different anomalies, connectivity problems, etc.) through 3D representation of computer networks. Specifically, we did realize 3D modeling and visualization of our university computer network with more than thousand devices. The purpose of three-dimensional representation of a network is to inform the network administrator in a real time for the problematic network devices in order to identify them. The real-time interaction between application and network administrator, gives the possibility to first disconnect alerted device from the network and then to access a right location for repairing or replacing the device. As an alternative method of data analysis, we think that 3D visualization is very useful.

REFERENCES

- [1] Goodall, John R. "Introduction to Visualization for Computer Security". Proceedings of the Workshop on Visualization for Computer Security, Springer, 2008, 1-17, Berlin.
- [2] The Open Scene Graph Website [Online], Available: <http://www.openscenegraph.org/>
- [3] B. Cheswick, H. Burch, and S. Branigan "Mapping and visualizing the internet". In Proceedings of the 2000 USENIX Annual Technical Conference, pages 1–12. USENIX, 2000.
- [4] B. Shneiderman. "The eyes have it: A task by data type taxonomy for information visualizations". In Proceedings of the IEEE Symposium on Visual Languages '96, pages 336–343. IEEE, IEEE Computer Society, 1996.
- [5] Stephen G. Eick and Graham J. Wills, "Navigating Large Networks with Hierarchies", Visualization '93 Conference Proceedings, San Jose, California, 1993, pp. 204-210.
- [6] Robert Ball, Glenn A. Fink, and Chris North, "Home-Centric Visualization of Network Traffic for Security Administration", ACM Conference on Computer and Communications Security, Workshop on Visualization and Data Mining for Computer Security 2004, (VizSEC 2004), pg 55-64
- [7] D. A. Keim. "Designing pixel-oriented visualization techniques: theory and applications". Visualization and Computer Graphics, IEEE Transactions on, 6(1):59–78, 2000.
- [8] C. Hundhausen, S. Douglas, and J. Stasko. "A meta-study of algorithm visualization effectiveness". Journal of Visual Languages and Computing, 2002.
- [9] C. North, B. Shneiderman. "Component-Based, User-Constructed, Multiple-View Visualization". *Proc. ACM CHI 2001 Conference*, pg. 201-202, (2001)
- [10] Erbacher, R. F. (2003). "Intrusion behavior detection through visualization". In IEEE International Conference on Systems, Man and Cybernetics, 2003., pp. 2507-2513, Albany Univ., NY, 5-8 Oct. 2003.
- [11] Matthew J. Pastizzo, Robert F. Erbacher, and Laurie B. Feldman, "Multi-Dimensional Data Visualization", Behavior Research Methods, Instruments, and Computers, Vol. 34, No. 2, 2002, pp. 158-162.
- [12] Robert F. Erbacher, Kenneth L. Walker, and Deborah A. Frincke, "Intrusion and Misuse Detection in Large-Scale Systems", Computer Graphics and Applications, Vol. 22, No. 1, January/February 2002, pp. 38-48.
- [13] Luse, Andy, "Exploring utilization of visualization for computer and network security" (2009). Graduate Theses and Dissertations. Paper 12042, Iowa State University. Available: <http://lib.dr.iastate.edu/etd>
- [14] B. Camaj, "Using 3D visualization to optimize a road construction", IJAST, Vol. 4, No. 7; December 2014. Available: <http://www.ijastnet.com/journal/index/693>
- [15] Tellenbach, Bernhard Martin, "Detection, classification and visualization of anomalies using generalized entropy metrics", Eidgenössische Technische Hochschule ETH Zürich, Nr. 20929, 2012. Available: <http://e-collection.library.ethz.ch/view/eth:7047>