

# Visualization of the Home Network

Zhihua Jin

Helsinki University of Technology

zhihua.jin@tkk.fi

## Abstract

Since modern home network is getting more complex, common users demand a handy tool to monitor the system every day so as to help them keep it usable and secure. Visual solution is suitable in this case but need to be designed with serious consideration of the human factors. Under the guidance of a generic value model for evaluating visualization, a new solution to visualize the home network is presented with the concerns of human factors. Then, some analysis is given for the new solution, followed with the future development direction.

**KEYWORDS:** visualization home network security usability

## 1 Introduction

Home computing environment is taking a more and more important role in common homes and connecting all the home computing devices within a home network is becoming the mainstream [5]. So, such network is required to work as reliable as other home appliances from the end users point of view. For the home network composed of more complex computing devices, suitable monitoring tool is needed so as to assist the management in a straightforward and comprehensive way.

Traditional techniques [1, 12] of monitoring and managing computer network are not applicable in the case of home network. They are usually used by professionally trained administrator who is responsible for a large complex network, while the users in our case could be of different ages, have different background, lack of professional knowledge in the field of computer network and security, and want to monitor a small home network so as to keep them working in the right way. The only same thing between the traditional network monitoring tool and the one in our case is that they are both expected to let their users notice the abnormal patterns of the network fast.

Therefore, new solution need to be developed specifically for home network, and visual method seems to be a suitable direction. To design new visualization solution and choose existing appropriate visualization method, guidance is needed. For the designing the big-picture visualization framework, the value model proposed by Wijk [13] is a good guidance. Besides the big-picture solution, detailed monitoring is also necessary, for which existing suitable visualization techniques should be chosen both based on the value model and human factors, and fitted into the big-picture

framework.

In this new solution, a home network is not only seen as the connections but also the connected entities. Monitoring and management is the main job of the solution, while making decisions and configure the home network is left for its users. How to implement the visualization is out of scope of this work.

Currently, there are already many information visualization methods [7], but not very well applied no matter in general or in specific field such as information security as expected [13]. Because first, there is still not a generic way to evaluate visualization methods; second, human perception and cognitive theory [14] is very important in evaluating the effect of visualization method, but unfortunately such theory is still not attracting much concerns in the application of information security monitoring. In section 2, related visualization work will be mentioned, especially the value model for visualization technologies.

In section 3, we will first explore what should be visualized in a home network environment, and then present the new solution on how to visualize the chosen components of a home network. Then in section 4, some analysis of the new solution will be given from the view of the value model and human factors, mainly about how well does our solution fulfill our initial objective and meet the actual requirements and how practical our solution is in consideration of current environment. Finally, a future development direction will be given for this solution in section 5 as a conclusion.

## 2 Related work

For this work, there are generally 3 main fields of related research, namely computer graph visualization technology, human perception theory and information security technology.

Graph visualization technology is the technical foundation of our work. As an independent field, it has been developed for 20 years since 1987. Towards the goal of helping people to get insight of the possible patterns or phenomena in massive amount of data set, various fantastic visualization methods [7] have been invented. Botanical visualization [8] is the choice of the framework visualization method in our solution. There are also other methods applied in the sub-visualization of the framework, which will be discussed more in the solution section.

Although information visualization is getting mature, it is still lack of handy measures and application methods. In other words, it is still not easy for people to choose suitable visualization method and apply them in their own work.

Wijk [13] proposed a model to help people evaluate the value of different visualization methods from a technological point of view, and pointed the importance of considering human factor in the field of visualization. Though his work mainly focuses on helping people understand and qualify visualization in general, it is also very useful in guiding people to choose and apply visualization techniques in practice. This work is basically guided by Wijk's value model [13] of visualization, and trying to take the human factor into account as much as possible.

As our visualization solution is designed for monitoring the home network, by which we hope to keep the home network secure, we are actually trying to monitor the abnormal and insecure phenomena [3, 5]. As a matter of fact, there are already many visualization tool that help administrating big network in use [1, 9, 12, 10]. For those methods, we need to acquire the useful techniques and experience from one hand, and modify them so as to fit them into our own need from the other hand.

Wijk's model [13] is coarse and abstract. We choose it as our guide not because it is proved correct but because it seems suitable in our case and we don't have many options. The same thing happens to other detailed visualization method in our solution. As general visualization methods, the value of this solution needs to be testified in practical use, rather in its design. In addition, as human factors might have more achievement in the future, our solution should be replaced with more suitable visualization solutions which are chose or created accordingly.

### 3 The tree-vision solution

#### 3.1 Objective behind the visualization

Wijk presented in [13] that we should evaluate the value of a visualization solution by first deciding what the objective behind it is. In the visualization of home network, our objective here is that by using the visualization tool, the home users could effectively and efficiently monitor the status of their home network, and make right decisions of taking any operation to it based on the pattern or phenomenon they have found in the visualization, in order to keep the network secure and usable.

Such objective can be decomposed into several aspects. First, most common users should be able to use such visualization solution, i.e., this solution should have the least common assumption of its potential users. In other words, the value of the solution should not base on the requirement to its users. Second, this solution should show the status of the home network in an effective and efficient way. As a result, the users should be able to get the important information of the home network from the visualization in a reasonably perception time. Third, the status information acquired by the users should be the one that could help them to make good enough decision of their further operation towards the network. Fourth, we use the solution to help us maintain the home network in a good status, i.e., secure and usable.

#### 3.2 What should be visualized

Although we mainly consider a home network as a single self-contained object in this solution, we still need to consider each entity of it separately. Basically, we can actually visualize everything in the home network. However, because we have limited resources to save and explicit objective to achieve, we should still only take the necessary parts which affect the usability and security of the network most into account.

Guided by the ultimate objective, which is security and usability, we consider a common home network and its secure problems as described in Ellison's [5], but from a system level. Assuming we have several desktop and laptop PCs, several common peripheral devices such as scanner and printers, several mobile handsets such as PDA and cell phones, some server such as web server and digital TV recorder, and all the necessary wired and wireless devices that connect all the previous devices and provide appropriate protection, such as router, switch, firewall, etc.

Generally, we could consider the home network from two sides: one is the entities connected by the network; the other one is the traffic and events happen on the network itself. For all the computing entities (mainly the PCs), we could visualize their physical health status (such as CPU temperature, cooling fan rotate speed, harddisk days of use, etc.), critical software status (such as antivirus software update records, personal firewall filter rules, etc.), general resource usage status (CPU, memory, disk space, bandwidth, etc.), and data usage status (file access control list, file access history, etc.). For the network traffic, we should visualize its dynamic statistics of throughput and characteristics (such as protocol type, destination, origination, port number, etc). Although most intrusions is related to the events in the network traffic, a combining of the events both in network traffic and computer software and hardware status are more useful in identifying security problems, because too much false alert could be reduced. Therefore, we also need to visualize such combination between network traffic and entity status.

#### 3.3 Big picture-the global visualization framework

As previously described, even though we have limited the scope of our visualizing objects, we still need to visualize a lot of stuffs. The efficiency requirement and resource limits (only one screen, for example) in our objective decide that we should be able to visualize as much important aspects of the network as possible in one big picture, where we can also dig into detailed visualization when we need to. In the theory of information visualization, it is a typical focus + context problem [7, 14], and there are several techniques to solve such problem. The framework in our solution is based on this focus + context theory and techniques. In addition, our objective also indicates that users of different background should be able to perceive the phenomena and retrieve necessary information. Since computer technology, especially computer security technology is not familiar to most people, it is necessary to transform these knowledge to another more common knowledge. Our solution framework is trying to do such transformation.

In this solution, a botanical tree as shown in fig. 1 is the common knowledge concept we chose as the framework visualization. The reason of such choice is very simple: we think that a botanical tree has very similar hierarchical structure as computer file system and computer network, which are two main objects we want to visualize. As science and technology often get inspired from the amazing nature, it might be easier to understand our technology in the view of nature. There are already some work showing practical use of such metaphor in information security system [6, 4]. Fortunately enough, we have existing techniques [8] to visualize huge hierarchical structure such as computer file system and computer network.

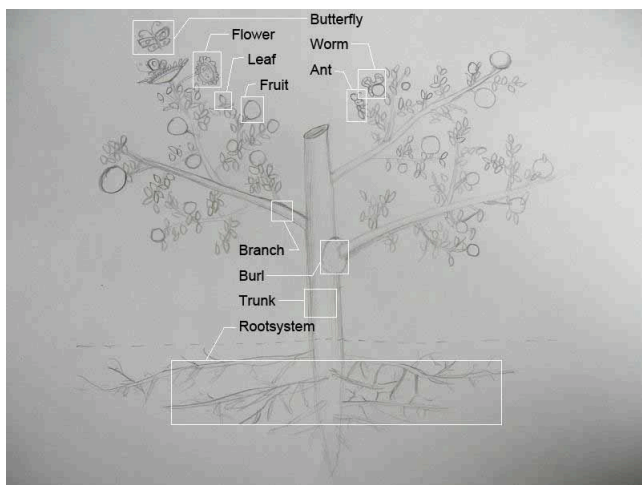


Figure 1: A botanical tree generated by computer [8]

When think of a normal tree in real life, we know there are mainly two parts of it: the branches, leaves, flowers and fruits above the ground, and the root system under the ground. Of course, we also have the trunk that connects those two parts. The following is a coarse mapping of each part of the tree to a home network.

- **Branch**

Every embranchment of a branch from the trunk could represent a single computing device. Global status such as physical health and resource usage could be shown on the surface of the main branch, while the whole file system could be mapped onto the sub-branches.

- **Leaf**

There are usually many system and application files in a PC. Those files are important to keep the system functioning normally, but seldom accessed by end users. If we map them to the leaves, we should mainly focus on the integrity and existence of those files, which can be easily shown by the surface color or texture of the leaves. The shape of leaves could be also used to differentiate the system files and the user application files.

- **Flower**

Most PC system at home may more or less have some network services. In addition, many user applications might work as a network service. Those services are critical to network security and need real time monitoring. Besides in nature flowers are considered as the attractive caffè serving small insects such as bees and butterflies, we decide to use flower to represent such services. For example, shape can be used to differentiate the type of service, size can show the capacity, and color can show the security level.

- **Fruit**

Fruits are usually assimilated to the productions of people's hard work. In fact, people become more and more likely to store their work in their computers. Normally, people want their work to be well protected according to their needs. For example, some classified files are not supposed to be access by unauthorized users, and some files could only be read but not modified by other users. For those critical data, we map them to the fruit of the tree. Shape, color, size can be used to represent their owner, size, security level. More detailed properties of the file such as access control list and access history will be discussed in the section of sub-visualization.

All the over-ground objects of the tree should avoid covering their peer objects as much as possible when seeing the tree from the top, as the real trees do.

- **Root system**

A root system gives people a sense of reticular. So does the network traffic. Although a home network is a network itself, its main network traffic is usually not within the intranet but between the intranet and the Internet. This is one of the main factors that bring in the security problems to home network. If we use the root systems to represent all those traffic and see through the ground from the top view, the traffic from external network will converge to the center, where lays the local home network. This traffic map is already a popular method in network monitoring techniques to show potential pattern in complex network environment. We will discuss more about this issue in the sub-visualization section.

- **Trunk**

As root system is assigned to represent the network traffic between internal and external network, a trunk seems quite suitable to represent the network traffic within the local network. Since showing all traffic will be overwhelming and unnecessary, we only use the diameter of the trunk and main branches to represent the overall throughput in default mode. When the traffic of a segment is over a predefined threshold for a predefined time, a burl will grow in the crotch. Detailed traffic will be represented by tracheas inside a trunk. By applying other visualization techniques, we may visualize the connection between the system status and traffic status, which is very effective to identify abnormal events.

A tree lives in an ecosystem in real life, which means it lives with other species, such as bees, butterflies, ants, worms, etc. In fact, there are also amazingly identical little companies for a home network. For example, bees and butterflies enjoying the honey in flowers are identical to client

users consuming the network services. Worms living around the root system is identical to worms spreading in the network. Ants eating worms is like antivirus software searching and eliminating virus and worms. In a word, a virtual tree in a screen can show many security and usability critical phenomena of a home network in an effective and efficient way.

### 3.4 Sub-visualization

As botanical tree visualization [8] is the top level field of vision for users to grasp the overall status of the monitored home network at a glance, more subvisualization methods showing detailed local characteristics are still needed for further examination when users found interesting phenomena in the big picture that worth looking into. From the focus + context point of view, it is time to focus.

There are many ways to solve the focus + context problem [7] such as the fisheye distortion technique that zoom in and accentuate the focused region. In our solution, we mainly use the zooming, toolglass and magic lenses [2] methods to transit between the global vision and local vision. A toolglass is a transparent moveable tool bar from which user can click and use some tool presented on the glass, while the magic lenses are different vision layers showing the same observing object from different angles. Assuming a user found a burl coming out on the branch or on the trunk, he/she could zoom in to the burl area, choose the see-through view mode from the toolglass that shows up in a focus mode, and then see through the surface of the trunk and find more detailed information of the abnormal traffic which mapped to the trachea of a tree. In addition, the tree is represented in a fixed 3D space, where the normal 3D graph operations such as zooming and rotating could be applied. Thus, by 3D graph operations, users can also have different vision of the tree.

After the transition phase, users will get into a sub-visualization mode. Since the tree visualization is considered as the framework for the sub-visualizations, those sub-visualization methods should keep consistent with the tree related visual concepts as much as possible, though the elements such as leaves and branches could slightly change their shape and be reorganized according to different purpose. For example, in system data integrity, leaves are organized mainly by the structure of file system. But when user change to user data history view, the leaves will be reorganized mainly by the pie graph which indicates access control. During such reorganization, branches connecting leaves needs to be stretched accordingly. As user use sub-visualization mode to find functional problems, we sort them by function other than by botanical structure.

- **System data integrity**

When choose this option from toolglass and see from the top of the tree, a magic lens will be applied to shield (or blur) other objects and only show the leaves and branches which may degenerate to lines. Since leaves naturally spread around the branches, and shows the integrity status of the represented file by color, it is very easy to see if some system or application files have been modified. Besides, since files of different system modules or applications could be

sorted on different vertical levels of the tree, it gives users a convenient way to navigate the files.

- **User data access control**

When choose this option from toolglass and see from the top of the tree, a magic lens will be applied to shield other objects and only show the fruits. The access group could be represented by the color, and the allowed operations could be represented by the shape.

- **User data history**

To visual the access history of each file, a rings and ripples method similar to the one created in [11] is applied here. As shown in fig. 2, different sectors represent different system(PC) in the home network which belongs to certain users(mom, e.g.). Different ring cirques of a transparent pie graph in the top view of the tree represent different allowed operations of the file with different colors. All fruits will be reallocated in such corresponding ring cirques of the pie, where the closer the fruit is to the center, the more critical operations are allowed. More over, if a file is accessed by a user, a ring will be shown around the edge of it. The operation of the user will be shown by the color of the ring which is corresponding to the ones of ring cirques. Thus when an illegal access request is recorded, it will be very easy to notice. Besides, old access history rings will disappear after a predefined time or number, which can imply the popularity and potential danger of a file. Though the history wears are represented as rings here from a 2D topview, they are actually transparent color layers in 3D space. Therefore, when seen from the big picture, an element looks darker if it has been frequently accessed by different users, or it may become close to the color of a user if it is mostly accessed by this user.



Figure 2: User data history pie graph

**Services access control** and **Services access history** is

very similar to user data, only that the main role fruit is replaced by flower.

- **Local network traffic metrics**

When choose this option for a local traffic segment such as a part of a branch, a normal dynamic throughput analysis of different protocols will be shown as the different tracheas inside the branch. Color represents protocol, while thickness represent the amount of throughput.

- **Global network traffic matrix**

When choose this option, a top view magic lens will focus on the underground root system. Resembling to the matrix seen in other popular network monitor tools such as SnifferPro, this matrix is a line graph that shows the connections between the local hosts and the external ones, where all local hosts lie in the center of the graph while the external hosts lie on the round edge of the root system.

- **Firewall status**

When choose this option for an interface between the main branches and the trunk or between the trunk and the root system, where a firewall presents, the view changes to such interface and a magic lens is applied to visual the firewall by a method presented in [1]. As shown in fig. 3, we map all the connections to a pixel to a pie graph similar to the one we mentioned for the user data. Each pixel falls on a specific ring cirque of the pie, where the closer the pixel is to the center, the more trustable the connection is. Different sectors of the pie represent different system of the home network. The color of pixel could be used to show the protocol. When the cursor is on a certain pixel, more information of the traffic such as source/destination IP/port pair and protocol type will be shown on a pop-up pad.

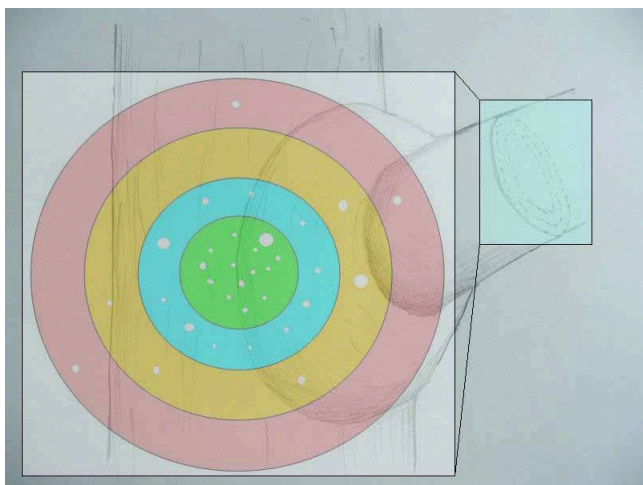


Figure 3: Firewall status pie

- **Global correlation traffic**

Because most of intrusions involve not only network traffic but also backend application, visualize such correlated

patterns could help effectively and efficiently identify the intrusion. As presented in [1] and shown in fig. 4, the network connection pixel map shown in Firewall status is used as the frontline of a connection between two hosts. Then each pixel will map onto the port plane behind it so as to indicate the port. Actually, with the help of toolglass and magic lenses, we could insert more intermediate planes such as protocol plane and IP plane in this case. Behind those intermediate screen planes, we have the application plane shows the characteristics of the backend application, such as socket type (client or sever) and socket status. This visualization could be activated when a traffic in any vision is selected and the corresponding option on the toolglass is selected. When a relation among network service from system directory, user application and data, and connection to outside host is shown as an attention-getting way such as a read line, the user should be suspicious and start digging for more details. Typical relation patterns could be provided by product supportor as update package similar to 'virus database update', which could be used by end users to find suspicious events. Or the end users could simply send screen capture to product supportor and left the rest of the work to the specialist.

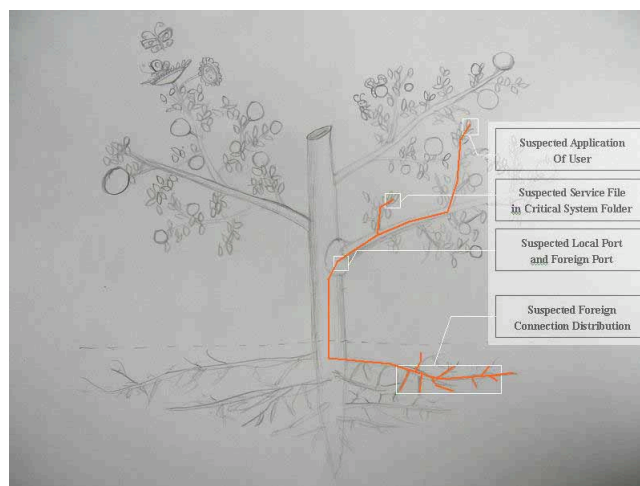


Figure 4: Global correlation visualization

## 4 Discussion

As this solution is guided by Wijk's model [13] and human perception theory [14], we will also examine the solution from those aspects.

First of all according to Wijk's model [13], how does the solution fulfill the objective behind it? As we have seen in the solution section, most of the important aspects of a home network are visualized in a pre-attentive and straightforward manner. That's to say, users can perceive the visualization quickly, and retrieve the knowledge from the perceived information regardless of their background. Moreover, since our visualization is highly objective oriented, the users can basically utilize the acquired knowledge to help them make decisions so as to keep their home network usable and secure, which clearly shows the value.

Now we can consider other factors of Wijk's model [13] such as initial development costs, initial costs per user, initial costs per session, and perception and exploration costs. Since most of the visualization techniques already exist, we don't have very high initial development costs. Because we only try to visualize the fixed objects of home network, initial specification of the visualization should only need to make once. Thus even we have high initial costs per session, we will not have very strong impact from it. As described in the solution section, this solution is designed under the guidance of human factors, perception and exploration costs should be reduced to a considerably low level. As this solution is for everyday use for normal home users, many users will use such solution, and so reduce the average initial costs per user. In addition, high user number and high using frequency will obviously increase the total positive value created by the solution. As a result, this solution should be valuable.

From the human perception point of view, the most benefit is the large utilization of visual graph. Research shows that human beings can identify an image in a very fast speed. For instance, normal people can easily find out if one special image is among a large amount of other images which shows in a frequency high enough to prevent the people from seeing any details of the images. The big-picture of this solution can easily exploit this phenomenon. The dynamic visualization of the tree picture could be recorded for every day. When the user is back home and want to see what has happened to the home network, he/she just need to replay the video record at a reasonably fast speed at which abnormal could be noticed easily. This way should be much efficient than the traditional text-based method.

## 5 Conclusion

In this work, we propose a visualization solution for home network. The solution consists of two parts, big-picture tree visualization as the framework, and sub-visualizations as assistant functional tool. This solution is supposed to be easy to use by all kinds of normal users in everyday life and effectively and efficiently monitor their home network, so as to help them make informative decision to maintain their home network in a usable and secure status. Human factors are the most concern in the design of this solution. However, as implied in [13], the value of any visualization method is not revealed by its design, but by its impacts in practical use. Thus, implement the solution and get experimental result is still the best way to examine this visualization solution. If this solution is proved to be good in monitoring, more future work may be focus on how to combine the monitoring and configuration together.

## References

- [1] R. Ball, G. A. Fink, and C. North. Home-centric visualization of network traffic for security administration. In *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 55–64, New York, NY, USA, 2004. ACM Press.
- [2] E. A. Bier, M. C. Stone, K. Pier, W. Buxton, and T. D. DeRose. Toolglass and magic lenses: the see-through interface. In *SIGGRAPH '93: Proceedings of the 20th annual conference on Computer graphics and interactive techniques*, pages 73–80, New York, NY, USA, 1993. ACM Press.
- [3] CERT. Home network security, 2006.
- [4] P. DiGioia and P. Dourish. Social navigation as a model for usable security. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security*, pages 101–108, New York, NY, USA, 2005. ACM Press.
- [5] C. M. Ellison. Home network security. *Intel Technology Journal*, 6(4):37–48, 2002.
- [6] W. Harrop and G. Armitage. Real-time collaborative network monitoring and control using 3d game engines for representation and interaction. In *VizSEC '06: Proceedings of the 3rd international workshop on Visualization for computer security*, pages 31–40, New York, NY, USA, 2006. ACM Press.
- [7] I. Herman, G. Melancon, and M. S. Marshall. Graph visualization and navigation in information visualization: A survey. *IEEE Transactions on Visualization and Computer Graphics*, 6(1):24–43, 2000.
- [8] E. Kleiberg, H. van de Wetering, and J. J. V. Wijk. Botanical visualization of huge hierarchies. In *INFOVIS '01: Proceedings of the IEEE Symposium on Information Visualization 2001 (INFOVIS'01)*, page 87, Washington, DC, USA, 2001. IEEE Computer Society.
- [9] K. Lakkaraju, R. Bearavolu, A. Slagell, W. Yurcik, and S. North. Closing-the-loop in nvisionip: Integrating discovery and search in security visualizations. In *VIZSEC '05: Proceedings of the IEEE Workshops on Visualization for Computer Security*, page 9, Washington, DC, USA, 2005. IEEE Computer Society.
- [10] E. L. Malcot, M. Kohara, Y. Hori, and K. Sakurai. Interactively combining 2d and 3d visualization for network traffic monitoring. In *VizSEC '06: Proceedings of the 3rd international workshop on Visualization for computer security*, pages 123–127, New York, NY, USA, 2006. ACM Press.
- [11] J. Rode, C. Johansson, P. DiGioia, R. S. Filho, K. Nies, D. H. Nguyen, J. Ren, P. Dourish, and D. Redmiles. Seeing further: extending visualization as a basis for usable security. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 145–155, New York, NY, USA, 2006. ACM Press.
- [12] R. S. Thompson, E. M. Rantanen, and W. Yurcik. Network intrusion detection cognitive task analysis: Textual and visual tool usage and recommendations. In *Proceedings of the Human factors and ergonomics society (HFES) 50th annual meeting, 2006*, 2006.
- [13] J. J. van Wijk. The value of visualization. In *Visualization, 2005. VIS 05. IEEE*, pages 79–86, 2005.

- [14] C. Ware. *Information Visualization: Perception for Design*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004.