

# Glyph-Based Generic Network Visualization

Robert F. Erbacher  
Department of Computer Science, LI 67A  
University at Albany-SUNY  
1400 Washington Avenue  
Albany, NY 12222, USA  
erbacher@cs.albany.edu

## Abstract

Network managers and system administrators have an enormous task set before them in this day of growing network usage. This is particularly true of e-commerce companies and others dependent on a computer network for their livelihood. Network managers and system administrators must monitor activity for intrusions and misuse while at the same time monitoring performance of the network. In this paper, we describe our visualization techniques for assisting in the monitoring of networks for both of these tasks. The goal of these visualization techniques is to integrate the visual representation of both network performance/usage as well as data relevant to intrusion detection. The main difficulties arise from the difference in the intrinsic data and layout needs of each of these tasks. Glyph based techniques are additionally used to indicate the representative values of the necessary data parameters over time. Additionally, our techniques are geared towards providing an environment that can be used continuously for constant real-time monitoring of the network environment.

**Keywords:** Information Visualization, Computer Networks, Traffic Monitoring, Intrusion Detection

## 1. INTRODUCTION

Large scale telecommunication infrastructures provide the foundation on which e-commerce and other computing applications are based. However, monitoring such large scale systems to determine the effectiveness of the current infrastructure is a daunting task given the complexity of current infrastructures and interactions between the systems and user based traffic. There is a need to monitor activity on many levels simultaneously; all of which are considered critical to today's commercial needs. The most obvious requirement is that of intrusion detection. We have been applying visualization techniques towards the identification of intrusions and misuse through the identification of behavioral patterns. In this way, the system administrator can monitor activity on an entire network through a visual interface, which is much less tedious than the typical textual based interface commonly used. All network accesses by users are represented visually such that the temporal and system based relationships are shown instantly with the more important attributes highlighted to attract the attention of the system administrator. By observing the animation over time it is straight forward to identify the activity of individual users, how they are accessing the systems, and identify any irregularities. This should allow attacks to be identified and counteracted before they are successful.

The goal is to extend that basic philosophy to additional network information critical to the system administrator. By providing all relevant information in a single display we will be reducing the context switching necessary for analysis of relevant information and provide a more clear and meaningful representation of the information while also showing the relationships between the different data types. In particular, we are incorporating network traffic information, relevant to bandwidth usage analysis, within the intrusion detection monitoring environment. The need for intrusion detection monitoring should be clear. Traffic monitoring is also critical to today's infrastructure as it can identify bottlenecks preventing users or customers from accessing an organization's network based resources. The combined environment can show relationships between these two aspects of network traffic and aid the system administrator in resolving additional

questions of relevance; is identified network congestion the result of an attack, misuse, or an inappropriate network infrastructure organization?

## **2. MOTIVATION**

Visualization provides an effective mechanism for monitoring traffic patterns and evaluating the traffic patterns as they relate to the current infrastructure, particularly in the identification of bottlenecks, failures, and wasted resources. This becomes of particular value when rapid assessment is needed. Computational or log based mechanisms for analyzing such systems can require substantial time to perform the analysis and are often used in current scenarios to determine, after the fact, what went wrong. Our visualization techniques enable the analyst, by invoking the power of the human visual system, such that the state of the infrastructure can be identified instantaneously, providing immediate feedback if problems should occur. This would then allow the analyst to identify and implement a solution before customers or other users of the infrastructure become impacted by the problem and react negatively. Such problems can occur during localized periods of exceptional loads, failure of infrastructure components such as routers, denial of service attacks, internal misuse, etc.

The visualization techniques we are developing provide a dynamic view of the localized network infrastructure in conjunction with information on remote access, system load, system accesses, log information, and network topology. We use perceptually based representations that are easily understood and allow problems to be immediately identified. This is done using a glyph based approach that allows information from multiple sources to be combined into a single visual display and automatically correlates the information. The environment, at its basic level, provides details relating to the criticality of systems, network load and capacity, local and global peaks, system access log details, and temporal relationships of the bandwidth usage.

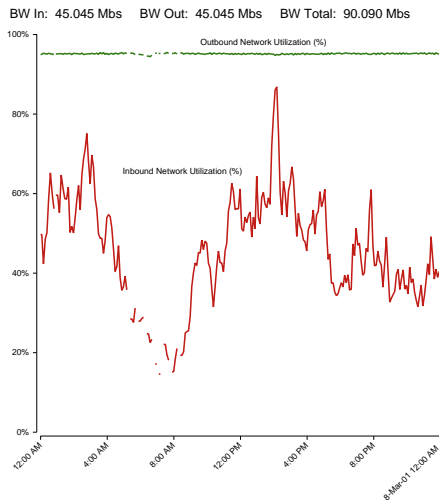
In commercial applications it is critical that customers have fast access to the organization's web sites. Should access be limited due to poor performance then the network managers must be able to identify the cause and source of the problem such that it can be corrected. This may be the result of insufficient capacity for the number of transactions, internal misuse in which employees are downloading material not relevant to their employment, or external misuse geared directly towards disrupting the day to day business of the organization. An effective and efficient environment is needed to assist in the monitoring of the network infrastructure such that the administrator can monitor the network and identify problems before they are noticed by customers. This must all be done while the administrator is performing other typical duties.

## **3. BANDWIDTH USAGE DATA**

Analysis of log information for the university's primary UNIX server reveals that there are as many as 200 users accessing the system simultaneously. During a one week period there are more than 25000 successful connections from over 2500 different hosts. The university's primary UNIX server provides e-mail and compute resources for the university at large. However, the university's network infrastructure is insufficient to handle this connectivity load, providing 10 Mb/s connectivity with 100 Mb/s connectivity in areas with specific needs. External connectivity provides 100 Mb/s.

The issue that arises is the determination of bandwidth usage through each network and subnet. Are there subnets that are constantly saturated or exceed their bandwidth capacity? Are there subnets that achieve localized peaks that exceed capacity? If so, why and when? What subnets are under utilized? Is all utilization related to university activities? What type of traffic is generated? Would it make sense to move resources closer to the external network connection or off-site, e.g., HTTP sites? These details are critical for management of the network infrastructure. The answers to such questions will aid an organization in determining how to reallocate bandwidth, determine where upgrades are required, and identify inappropriate usage. The goal is to provide better connectivity overall for the entire organization, its employees, and customers.

Typical network usage consists of textual summaries. This summary describes the network usage for a single subnet. Such textual representations can provide overviews of network usage. Fully managing the network from such summaries would require an enormous amount of time due to the difficulty in discerning relationships and meaning from text. Currently, the summary is only provided once per day. Full analysis would require the summary be provided at regular intervals, e.g., hourly or minutely. Summaries would then need to be provided for all sub networks as well as the network as a whole. The volume of textual information that would subsequently be generated would make the analysis process unfeasible.



**Figure 1:** Network usage graph.

It is also common to use basic line graphs to show bandwidth usage as is done by the network managers at the university, figure 1. The graph shows overall usage of the external network connection over time. It is clear that the university’s outbound network connection is completely saturated with no break. This has proven detrimental to students attempting to access the university’s resources from external locations. However, the graph does nothing to identify the network usage internal to the university. While the graph has been used to qualify the need for upgrading the external bandwidth, what about the internal bandwidth? Additional information is needed to facilitate the development of long range plans for network infrastructure upgrades throughout the entire university.

The network congestion brings up another issue, namely, how usable is the university’s connectivity for the student population? Individuals who are internal to the university’s subnet are able to access the university’s resources without too much difficulty. However, individuals who attempt to connect from the outside will find that there are significant delays when attempting to perform even the simplest task. There can be delays of 5-10 seconds before keystrokes are echoed onto the remote terminal. As the graph shows, this is not a matter of getting the input from the remote user to the system but rather getting the results of the input back to the user on the remote system. These limitations on student access to the university’s resources led to the desire to improve bandwidth through upgrades to the network infrastructure.

#### 4. SYSTEM LOG DATA

Currently, system administrators are required to analyze log files to identify an attack. These log files can incorporate millions of messages per day. The amount of data available results in system administrators not fully collecting or monitoring all available information for all systems under the administrators control, rather focussing on primary systems and servers and examining minimal information from the remaining systems. In fact, system administrators in general do not collect or analyze any data related to Microsoft or Apple based operating systems at all; even though it is possible for these systems to be the targets of break-ins, subversion, and misuse. Network traffic itself is only analyzed intermittently. Log file analysis is the greatest time consumer for system administrators if it is even done. Identifying actual intrusions and misuses requires that the intentions of the user be known during examination of the user’s activity. This is currently unfeasible and results in missed attacks and many false alarms. This situation is only likely to get worse and with the globalization of e-commerce and interest in Internet voting the potential for serious damage increases as well. Ultimately, the goal must be to identify an attempted break-in or attack before the attack is successful so that the situation can be monitored and a response initiated before harm occurs, in the case of a successful attack. Current log file analysis only reveals that an attack has occurred in the past. At this point it may not be possible to determine if the attack was successful or not since hackers generally subvert the log reporting facilities as one of their first actions. This leads to extensive amount of analysis being required to determine the integrity of each system. It is imperative that we reduce the number of false alarms and increase the number of true attacks detected.

## 5. PREVIOUS WORK

Most previous work on visualizing network data has been based on measuring performance or bandwidth characteristics. Very little prior work has dealt with visualizing network intrusion data, particularly real-time network intrusion data, as is our ultimate goal. We are attempting to visualize the actions of an enterprising hacker actively seeking to counter the attempts being made to identify that hacker's actions. This dynamism is an attribute that alone requires novel solutions.

### 5.1. Intrusion Detection Systems

Aside from our ongoing work in this area little prior activity has been applied to the use of visual analysis as an aid to intrusion detection. For instance, many have proposed use of a simple "odometer-like" or metered scale to indicate the estimated level of attack a system is enduring. This is embodied in the Hummer "perceived level of threat"<sup>1</sup> indicator. Earlier systems, such as DIDS<sup>2</sup>, provided graphical representations in the form of color to indicate when a system had experienced a sequence of suspicious events. While useful, these approaches do not provide adequate detail to do more than observe that attacks are in progress and do little to aid diagnosis. Frincke has performed preliminary investigations towards identifying likely models for depicting system state.

Data collection and filtering techniques have greatly aided the analyses; however, examination of both commercial and research efforts to identify security violations consistently generate considerable quantities of data—usually far too much to be evaluated effectively using current techniques<sup>3</sup>. Some of this is due to the way that data-gathering choices are made<sup>3</sup>. Refinements in the data gathering decision-making process will not suffice: as networks grow larger, the amount of misuse-relevant data will also grow. Hence, better methods for analyzing the data are needed, rather than continued reliance on primarily textual techniques.

### 5.2. Visualization systems

In contrast to intrusion detection, quite a bit of visualization research has been applied to network accesses. The principal body of work related to network intrusion is from the information exploration shoot-out, organized by Georges G. Grinstein and supported by the National Institute of Standards and Technology (NIST)<sup>4</sup>. In this project, researchers were given access to a data set consisting of network intrusions. The idea was to identify which researcher's techniques were effective at identifying the intrusions. The driving philosophy was that little work has been done to compare visualization techniques in a formal setting. Perceptual studies have been done to identify characteristics of the human visual system that should be used as a basis for the development of visualization techniques, but little has been done to actually compare and contrast visualization techniques. There is no body of literature that identifies what visualization techniques definitively work better on a given data set.

Most previous work involving visualization related to networks has emphasized graphics that depict network performance and bandwidth usage<sup>5, 6</sup> even down to the router<sup>5</sup>, individual packets, and individual e-mail messages<sup>7</sup>. The techniques developed for these purposes do not provide sufficient detail or handle sufficient numbers of nodes and attributes in combination for our needs. The work by Eick et al.<sup>7</sup> strictly deals with e-mail and subsequently resolves many fewer nodes and attributes than is needed for intrusion detection. Other work has been geared towards visualization systems for program analysis and program development. These environments typically deal with small numbers of processors that are working on a single task and thus have a common grounding. This research into network usage has not been applied to network intrusions.

Becker et al.<sup>8</sup> discuss the SeeNet environment that provides linkmaps for visually representing the amount of data being sent between two network nodes. It can identify when a node is overloaded, shows the network's behavior, how data moves between locations and its volume. This is critical during a crisis and usage increases, e.g., after a California earthquake. Understanding the consequences of events, so that, for example, telephone companies can be prepared for changing demands, is imperative.

Livelink<sup>9</sup> is an environment for visualizing and measuring the web. By probing web accesses they gather statistics on the number of hits web sites are receiving. This statistical information is presented in visual form as charts and graphs. An extension to the environment provides a more advanced graphical representation. In this advanced form, the approximate location of network nodes is represented, showing geographical association between web sites. The visual representation of each node is then presented in such a way as to reveal the activity of the site. Each node can represent several parameters simultaneously.

Netmap<sup>10</sup> is a generic visualization tool for the representation of relationships within a data set. The environment is principally geared towards showing known relationships of static data sets. Netmap is not geared towards exploratory data analysis in which the relationships are unknown and must be identified, or for temporally changing data sets. In contrast, it is the unknown nature of intrusion data that is the driving force behind the visualization techniques we are developing.

Finally, the work by Estrin et al.<sup>11</sup> is designed to visually simulate individual packets to aid in the development of protocols. It does not deal with visualization of the network at large and the issues developed once a protocol is deployed and the effectiveness of the network must be measured overall. The techniques do incorporate more realistic node placement, though on a very small scale. With the advancement of graphing theory and algorithms<sup>12</sup> developing appropriate node placement algorithms should prove feasible for our environment as well, even when dealing with huge numbers of nodes.

A major divergence of this work from much of the prior work is its focus on simple 2D techniques geared for continuous online monitoring of the network by system administrators and network managers. The ultimate goal is for the creation of a new body of techniques usable by system administrators in conjunction with all of the other tools in their toolbox which they maintain on their graphical display for administrative tasks. Many current techniques, incorporate 3D techniques which make them unsuitable for continuous monitoring, are difficult to understand for our target users, are not suitable for continuous monitoring as they require too much screen real-estate, or require frequent interaction.

## 6. VISUALIZATION TECHNIQUES

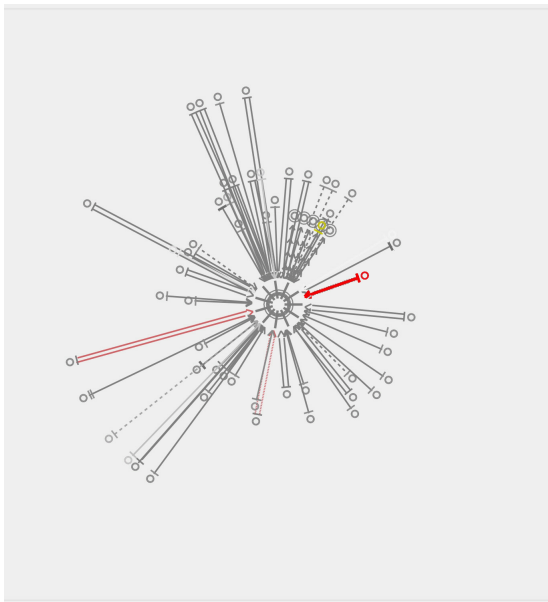


Figure 2: Intrusion detection visualization.

The question then remains, given the network data, relating to bandwidth usage and system log files, how can we combine all of this information into a single visual display such that it is easily comprehensible by system administrators, showing all of the appropriate details and relationships. Clearly, the number of parameters in such combined data sets will be incredibly high and typical techniques won't work satisfactorily. To this end, we have developed glyph based techniques geared towards multidimensional data visualization. The techniques incorporate sufficient attributes to fully represent all of the relevant parameters from the originating data sources. The glyphs themselves are organized on the screen based on their locality and criticality.

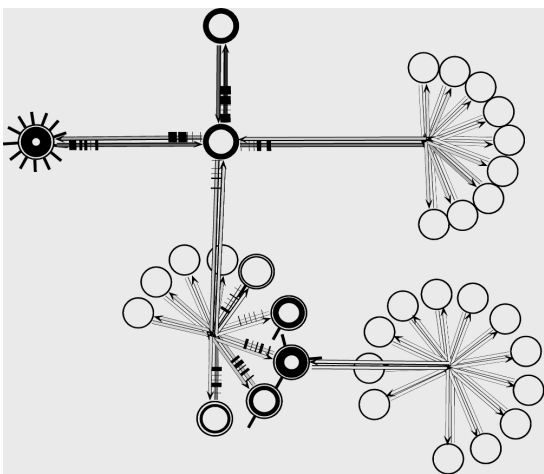
### 6.1. Intrusion Detection Visualization

Figure 2 shows an example of our intrusion detection visualization<sup>13</sup>. The environment shows the system being monitored in the center of the window and connecting systems in concentric circles around the monitored system. The ring in

which a node is placed is representative of the difference between the IP addresses of the monitored system and the connecting system, providing a representation of locality.

The monitored system has additional information attached to its representational glyph. Namely, each spoke is representative of ten users and the thickness of the inner circle is representative of the system load. The connecting nodes have cross hashes representing the number of different users connecting from that node, individual cross hashes, and the number of connections by that user, thickness of the cross hash,

The directed lines are themselves glyphs showing the direction of the connection, the state of the connection, and the type of connection. A node with two parallel lines is indicative of an unauthenticated connection. If the parallel lines are red then the authentication has failed. Solid lines are telnet or rlogin connections, long dashed lines are privileged ftp connections, and short dashed lines are anonymous ftp connections. Lines with multiple arrows, usually four, are indicative of NFS connections. A lost NFS connection is represented by highlighting the node in yellow. Thick red lines represent port sentry identified attacks.



**Figure 3:** Network bandwidth visualization.

## 6.2. Bandwidth Usage Visualization

Figure 3 shows the network bandwidth usage environment<sup>14</sup>. This environment grew out of the work on intrusion detection work and the realization that no simple network monitoring environments exist for system administrators or network managers to use continuously in an online fashion. The main difference between this visualization and the system attack visualization is the need to incorporate intermediary nodes within the visual layout that are usually not of interest. This visualization shows a small subnetwork within the university. Two routers are present as well as three switches/hubs.

The routers are represented by glyphs composed of circles with a single thick ring. Switches and hubs are represented by the joining of network connections. This implicit representation is a natural fallout of the inability to collect network specific data from switches and hubs, as can be done with routers or smart switches.

As with the attack visualizations the network bandwidth visualization incorporates glyph based mechanisms for representing parameters relevant to bandwidth analysis. When available spokes are used to represent the number of users on the system and the thickness of the inner ring is used to represent system load. The hash marks are used to represent the amount of different types of traffic. The thickness of the hash mark is representative of volume. The order of the hash marks is as follows: Ping, NFS, Telnet, HTTP, TCP, UDP, SNMP.

## 6.3. Integrated Visualization Requirements

The organization ultimately must integrate two divergent tasks. Namely, intrusion detection which must handle large numbers of systems, including remote systems, and show accesses between these systems in a virtual network fashion, the underlying network topology not being of critical importance. Second, network bandwidth usage which is principally focused only on local infrastructure and requires strict adherence to network topology in order for the meaning to be adequately comprehended. These two tasks can be represented simultaneously by integrating two views within a single display. Thus, the local topology and relevant systems are shown in the center of the display with all available attributes represented for each glyph. The outer portions of the display incorporate systems which are not local and few if any attributes are available. By representing the interconnections between the local and non-local systems differently it becomes inherently clear which systems are local and which interconnections are following the strict network topology.

The change in representation between local and non-local systems aids in dealing with scalability issues. The glyphs associated with non-local systems need not provide all of the visual attributes needed for local systems, since the associated parameters are not available for non-local systems. Since the log files we are dealing with can have connections from over 2500 different hosts we must be able to represent at least that many nodes on the screen simultaneously such that they can be differentiated.

It is important to mention the importance of our expected user base when developing the visualization techniques. Our user base is expected to be system administrators, network administrators, and security experts. Looking at the needs and expectations of these users was critical in driving the resultant implementation. We dealt strictly with 2D representations since navigating a 3D field would be too tedious given that the network monitoring would only be a one of many activities these users are involved in. Also, our user base may not be as accepting of such an interface, since all their other interfaces remain in the 2D. Our goal was to design an environment which the administrator could place in the corner of the screen along with any other tools. The visualization can then be monitored right along with all the other displays. The ability to reduce the size of the visualization display and still gain meaningful information, was therefore, considered a great success. All of the details aren't available in the reduced view, however, general activity is distinguishable, as well as highlighted events. Scaling up the window resolves all of the attributes for greater examination.

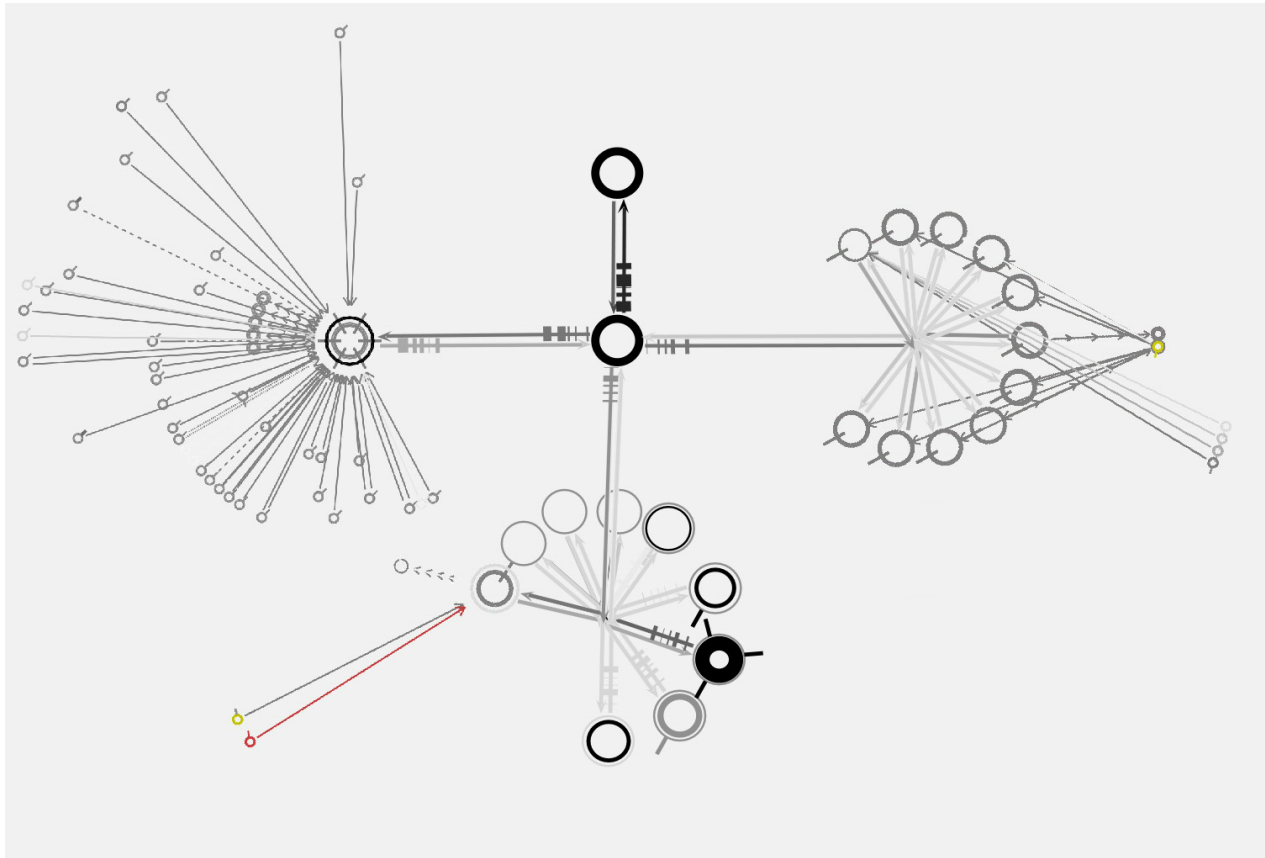
#### **6.4. Integrated Visualization Techniques**

In the current version of the environment, figure 4, we organize the layout in conjunction with the layout expected for the network bandwidth visualization. Using this layout as our basis we then build in the intrusion detection visualization. We connect nodes related to intrusion detection directly to the nodes to which the remote node has connected, ignoring the intermediary nodes. In order to represent this and also to related the concept that nodes are indeed local vs. remote we used very small nodes for the remote systems. We are careful to ensure that with the bandwidth analysis visualization all intermediary nodes are represented. The example in figure 4 shows only a small portion of the university network. The university network as a whole contains over 21 routers and over one thousand systems. Clearly there are scalability issues when attempting to display the entire university network which will need to be dealt with. This in general isn't a criticality as generally each subnet will have a separate system administrator, as with the computer science department's subnet. This greatly reduces the number of systems that must be monitored by any single system administrator. Additionally, while we limit the angle into which we place the remote nodes for the intrusion detection visualization we do not check for overlaps. The node placement consequently will require a more intelligent node placement algorithm in order to make the visualization more effective.

An additional issue is with that of the overloading of visual attributes within the glyphs. Notice that in both the intrusion detection visualization and network bandwidth visualization we have used hash marks along the connecting lines to be representative of data parameters. We felt it would be too confusing to users if we continued to use such a representation. We felt it would be better to use spokes on the remote nodes for the intrusion detection visualization to be representative of the number of users with active sessions as this would be more in line with our prior metaphor for users, the spokes representing number of users on the system. The use of the spokes still differs somewhat from the meaning for local systems. The spokes represent the number of users with connections and the thickness of the spoke represents the number of sessions by that particular user. The difference in the use of the metaphor is succinct enough that it should not lead to confusion. In conjunction with this and to reduce the screen real-estate required by remote nodes we greatly reduced the size of the remote nodes and their associated spikes. This difference in scale also aids in distinguishing between the context of the local versus remote hosts and subsequently the slight difference in meaning for the spokes.

#### **6.5. Visualization Analysis**

Examining figure 4 as an example of our techniques we can clearly see the remote versus local nodes. In conjunction with the local nodes the bandwidth usage is represented by the intensity of the interconnections. Separate interconnections are used to isolate the amount of bandwidth associated with inbound versus outbound traffic, an



**Figure 4:** Integrated visualization environment.

important consideration when attempting to decipher the importance of traffic on a network segment and the cause for significant loads. The volume of traffic associate with various protocols and the effectiveness of the network segment, e.g., ping time, is also clearly evident from the hash marks. When viewing the remote nodes, the volume of activity from each node is evident from the parameters mapped to the glyph, namely showing the number of users and the number of sessions maintained by each user. It is important to remember that the remote nodes are in fact traversing the network backbone through the university's network and contributing to the network load but for the sake of the analysis it is not relevant to show such detail rather leaving it implicit is sufficient.

The very center node of the visualization is the main university router. As is implied from the visualization, this router possesses many network ports, one for each subnetwork within the university. Only three of the subnetworks are shown in this example. Representing the university network in its entirety will encounter limited scalability issues. The problem will not be substantial since only a few nodes in the university receive large numbers of remote connections. The first such system is the university's main student compute server, which is shown on the left side of the visualization, essentially on a subnetwork of its own due to its high volume of activity. The second is the computer science departments main access point. All systems in the computer science department require that an individual already be on the department's subnetwork before they are allowed to connect to the individual systems. A single system in the department allows external connectivity. We are currently unable to collect data from that system directly. However, the implications of this setup can be seen from several systems representing the computer science departments subnetwork in the set of nodes at the bottom of the visualization. Namely, attempts to connect to the systems from the outside world fail, as indicated by the red and yellow nodes.

The right most group of nodes represents the UNIX based workstations in the university's main access computer lab. These systems are accessible from the outside world. However, being workstations and not servers it is expected that they should not be connected to but rather used directly from their console. The few connections that are present, all to the same machine in a very short period of time, would lead to some suspicion as to the motive of the connections. The node at the center top of the visualization is the router leading to the university's external network connection.

The layout of the nodes shown in figure 4 shows an effective extension of our original intrusion detection environment in which we only provided for the monitoring of a single system. Interrelationships between the local nodes must still be shown. Currently, if the same individual is connected to multiple systems this correlation will not be shown. In effect, each group, e.g. subnetwork, is maintained separately. This simplifies the maintenance and representational techniques, preventing substantial overlapping of nodes and interconnections. However, these relationships must be added in the future, in some way highlighting identical/duplicate nodes in different subnetworks, either continuously or when directly requested to do so for a particular node by the user.

In this combined environment, representing the system loads provides two analysis mechanisms. First, it aids in identifying heavily loaded systems in conjunction with high network loads to aid in the identification of performance or bandwidth bottlenecks within the infrastructure. Second, it can aid with intrusion detection. Systems will often achieve short duration peaks in which they are very heavily loaded. If a system is heavily loaded for a long period of time without a significant number of users or high bandwidth to back up this CPU usage then further analysis may be required. What is the user running which requires such a load? The user could have legitimate computational needs or could be attempting to crack the password file. As has been mentioned in our other papers on intrusion detection, this is just one identifier of possible untoward activity. Additional analysis will be necessary.

## 7. CONCLUSION AND FUTURE WORK

By visually representing the information associated with network and system usage and directly associating that information with the network layout our environment greatly enhances the ability for a network manager to assess the effectiveness of the network infrastructure and plan long range infrastructure management as well as deal with short term and immediate crisis, such as intrusions and misuses. The additional details the environment is capable of providing ensures that the available information is being put to the best use and provides the details needed to locate and eliminate waste and misuse should they occur. The power of glyphs to represent a vast number of parameters as visual attributes is a key to this capability. The visualization techniques make the network and system usage and limitations clear beyond a doubt.

An additional techniques we have begun examining is that of multiple views<sup>15</sup>. Multiple views provides the ability to easily integrate multiple techniques but does not meet our requirements of having a single display for continuous online monitoring. As an additional technique to gain additional insights once an anomaly has been identified multiple views will provide a useful capability.

While the intrusion detection capabilities are fairly robust the bandwidth monitoring capabilities are still very limited and only implemented in a limited prototype fashion. In order to make the environment truly useful we must improve the implementation all around and integrate data generated by much wider array of intrusion detection and network monitoring tools. In this way, our visualization environment will provide a visual interface to the results of associated monitoring tools.

## REFERENCES

1. Polla, D., J. McConnell, T. Johnson, J. Marconi, D. Tobin, and D. Frincke, "A Framework for Cooperative Intrusion Detection," *21st National Information Systems Security Conference*, pp. 361-373, October 1998.

2. Snapp, S. et al., "DIDS (Distributed Intrusion Detection System) Motivation, Architecture and An Early Prototype," *National Information Systems Security Conference*, 1991.
3. D. Zerkle et al. "A Data-Mining Analysis of RTID Alarms," *Recent Advances in Intrusion Detection*, Sept 1999.
4. Georges Grinstein, "Workshop on Information Exploration Shootout Project and Benchmark Data Sets: Evaluating How Visualization does in Analyzing Real-World Data Analysis Problems," *Proceedings of the IEEE Visualization '97 Conference*, IEEE Computer Society Press, Phoenix, AZ, pp. 511-513, 1997.
5. Kenneth Cox, Stephen Eick, and Taosong He, "3D geographic network displays," *ACM Sigmod Record*, Vol. 25, No. 4, pp. 50, December 1996.
6. Eleftherios E. Koutsofios, Stephen C. North, Russel Truscott, and Daniel A. Keim, "Visualizing Large-Scale Telecommunication Networks and Services," *Proceedings of the IEEE Visualization '99 Conference*, IEEE Computer Society Press, San Francisco, CA, pp. 457-461, 1999.
7. Stephen G. Eick and Graham J. Wills, "Navigating Large Networks with Heirarchies," In *Visualization '93 Conference Proceedings*, San Jose, California, pp. 204-210, October 1993.
8. Richard Becker, Stephen Eick, and Allan Wilks, "Visualizing Network Data," *Readings in Information Visualization: Using Vision To Think*, Stuard Card, Jock D. Mackinlay, and Ben Shneiderman, editors, Morgan Kaufman Publishers, pp. 215-227, 1999.
9. Tim Bray, "Measuring the Web," *Readings in Information Visualization: Using Vision To Think*, Stuard Card, Jock D. Mackinlay, and Ben Shneiderman, editors, Morgan Kaufman Publishers, pp. 469-492, 1999.
10. C. Davidson, "What Your Database Hides Away," *New Scientist*, Jan. 9, 1993, pp. 28-31.
11. Deborah Estrin, Mark Handley, John Heidermann, Steven McCanne, Ya Xu, and Haobo Yu, "Network Visualization with Nam, the VINT Network Animator," *IEEE Computer*, Vol. 33, No. 11, pp. 63-68, November 2000.
12. Giuseppe Di Battista, Peter Eades, Roberto Tamassia, and Ioannis G. Tollis, *Graph Drawing: Algorithms for the Visualization of Graphs*, Prentice-Hall, 1999.
13. Robert F. Erbacher and Deborah Frincke, "Visualization in Detection of Intrusions and Misuse in Large Scale Networks," *Proceedings of the International Conference on Information Visualization '2000*, London, UK, July, 2000, pp. 294-299.
14. Robert F. Erbacher, "Visual Traffic Monitoring and Evaluation," *Proceedings of the Conference on Internet Performance and Control of Network Systems II*, Denver, CO, August, 2001, pp. 153-160.
15. Jonathan C. Roberts, "Multiple-View and Multiform Visualization," *Proceedings of Visual Data Exploration and Analysis VII*, Vol. 3960, January 2000, pp. 176-185.