Network Intrusion Visualization with NIVA, an Intrusion Detection Visual Analyzer with Haptic Integration

Kofi Nyarko, Tanya Capers, Craig Scott, Kemi Ladeji-Osias
EVSC Laboratories, Morgan State University
nyarko@eng.morgan.edu, capers@eng.morgan.edu, cjscott@eng.morgan.edu, kladeji@eng.morgan.edu

Abstract

The explosive growth of malicious activities on worldwide communication networks, such as the Internet, has highlighted the need for efficient intrusion detection systems. The efficiency of traditional intrusion detection systems is limited by their inability to effectively relay relevant information due to their lack of interactive/immersive technologies. In this paper, we explore several network visualization techniques geared towards intrusion detection on small and large-scale networks. We also examine the use of haptics in network intrusion visualization. By incorporating concepts from electromagnetics, fluid dynamics, and gravitational theory, we show that haptic technologies can provide another dimension of information critical to the efficient visualization of network intrusion data. Furthermore, we explore the applicability of these visualization techniques in conjunction with commercial network intrusion detectors. Finally, we present a network intrusion visualization application with haptic integration, NIVA, which allows the analyst to interactively investigate as well as efficiently detect structured attacks across time and space using advanced interactive three-dimensional displays.

1. Introduction

In recent years, a huge amount of data has become widely available, owing to the wide spread use of computer networks. However, these networks are under constant attack by malicious users, creating a necessity for intrusion detection systems. These systems are an important component of defensive measures against malevolent users [1]. However, industry observers point out that today's intrusion detection systems, while useful, are not optimal [2]. Intrusion detection tools, which are generally based upon known attack signatures, cannot detect novel attacks. Additionally, they are not suited to the recognition of a structured attack that is distributed over time and across a very large network. Furthermore, they require sensors to collect massive amounts of data, which then must be sorted, analyzed, and displayed in a manner that separates interesting or suspicious events from normal network activity. Currently, this analysis process is very labor intensive and only rudimentary visualization techniques are used to display the results.

Visualization is a powerful link between the two most dominant information-processing systems, the human mind and the modern computer. It is a key technology for extracting information, and therefore it is becoming more and more necessary [3] in the field of network intrusion detection. The function of network intrusion visualization goes far beyond "illustration". Network intrusion detection can help to improve communication about the data to third parties; it can help the analyst to better explore specific properties of certain network attacks, and it can facilitate the exploration of distributed network attacks.

The near real time rendering of two or three-dimensional graphics on desktop computers and workstations bring to light many new and exciting ways to visualize network activities; especially anomalous activities such as malicious intrusions. One of the real challenges [4] in using advanced visualization technologies lies in choosing an optimal set of techniques and tools to illustrate anomalous network activity. Tools to visualize a variety of network activities through the use of advanced 2D and 3D rendering techniques will enable an analyst to interactively investigate suspicious activity within networks.

Traditional network analysis software and graphs cannot cope with the size of today's networks and their data collection capabilities. However, network visualization tools allow analysts to take in large amounts of information quickly, visually identify patterns in communication, and better understand causality [5]. While our powerful sense of vision has proven effective in most visualizing tasks [6], network intrusion visualization possesses many properties and relationships that may be

Proceedings of the 10th Symp. On Haptic Interfaces For Virtual Envir. & Teleoperator Systs. (HAPTICS'02)
0-7695-1489-8/02 $17.00 © 2002 IEEE

more effectively relayed through the augmentation of visual displays with haptic technology. Haptics is the name given to the process of feeling virtual objects. Our sense of touch, in combination with our kinesthetic sense, is capable of supplying a large amount of information about the structure, location, and material properties of objects.

We have developed a novel graphical tool with haptic integration (NIVA – Network Intrusion Visualization Application) for displaying and simulating forces involving network intrusion data. This tool employs display manipulation techniques that can help extract meaningful insights from the masses of network intrusion data currently available from today's network intrusion detectors (NIDs).

The aim of this paper is to examine visualization techniques in combination with haptic rendering utilizing NIVA in the context of protecting small and large-scale networks. Among other things, this paper addresses four important problems for visualizing large networks: (1) Positioning nodes, (2) Managing the links so they convey actual information, (3) Handling the scale of graphs with thousands or millions of nodes, and (4) Interacting with and navigating through large networks of information. This paper consists of four main sections. The first section (Section 2) outlines current network visualization methods related to network intrusion detection visualization. In Section 3 haptic visualization is briefly explored. Section 4 presents our network intrusion visual analyzer, NIVA. In this section we generally describe the tool and its features as well as display the relative effectiveness of the tool as a haptic visual intrusion detection analyzer. The integration of haptics into NIVA is explored in Section 5. Section 6 discusses the experimental procedure and results used to assess the benefit of the haptic interface. These benefits are further discussed in Section 7. Section 8 concludes with the direction of further research.

2. Related network visualization methods

Most NIDs have the ability to produce textual (tabular) output. Some have argued that data visualization simply substitutes for these tabular results, however, according to Chalmers [7], data graphics can do much more than simply substitute for tabular descriptions. At their best, graphics are instruments of reasoning about quantitative information. Often the most effective way to describe, explore, and summarize a set of numbers, even a very large set, is to look at pictures of those numbers. Graphical or visual presentations can not only describe data in different ways, but can also facilitate the comparison between different sets of data, stimulate scientific innovation, and even encourage theoretical insights.

Information visualization consists of an appropriate transformation of input data to output graphics [7]. Accordingly, it can be argued that a visualization method is acceptable, only if it clearly identifies the relevant information, defines an appropriate mapping, and generates the image accordingly. These three aspects are referred to as substance, design, and algorithm, respectively, which embody the general guidelines of network visualization

- Substance: when the network is conscious and precise about the information it intends to communicate and the means it uses to do so
- Design: The design of a visualized network is the specification of how its substance is mapped to graphical elements
- Algorithm: The procedure used to realize a design specification for the substance of a given network

Designing an informative and effective network visualization system can be a difficult task. However, this task can be simplified by adhering to certain design guidelines [3,8]. These guidelines provide a foundation for our approach concerning network intrusion visualization. The nature of our visualization approach can be described as task specific. By understanding the data analysis task, we ensure that the visualization is focused on the user's needs. For data analysis, a visual display is useful if it leads to insights and understanding, therefore our approach was developed with this concept in mind.

Network intrusion detectors inherently collect massive amounts of information, which must be processed, displayed and hopefully understood. Preferably in a visual system, this information is displayed as glyphs positioned on the screen in a pleasing, informative, and context-preserving arrangement. The best arrangements are perceptually linked to an important characteristic in the information, thereby facilitating the rapid transfer of information. In order to avoid clutter, it is essential for smaller size glyphs of appropriately simple geometric shapes to be used in conjunction with a reduced representation capable of displaying the entire information space on a single screen. For perceptual effectiveness, glyphs should be positioned in a way that seems natural for the dataset under study. Furthermore, the positioning should convey some essential and interesting aspect of the dataset, such as time, spatial information, or structure. By showing the complete database in a single view, it is possible to discover database-wide patterns. The most effective representations are those that make the patterns most obvious and perceptually salient.

Data encoding is the use of color and other visual characteristics to show the distribution of statistics in the database. Effective visual attributes for information coding are position, size, shape, color and motion. For quantitative comparisons, the most effective perceptual

data-encoding variable is size. Shape is useful for visual segmentation, although it is less effective for small glyphs. In practice, color, particularly when linked to interactive scales, works well with small glyphs, provided the color scale is carefully chosen.

As discussed earlier, network intrusion detectors produce large amounts of data that when displayed collectively, produce severe clutter even with the reduced representation overview. However, interactive filters can reduce the visual complexity by not displaying particular data items, thereby focusing on the interesting and informative patterns in the data. Effective filters include interactive color scales, linked histograms, and double-edged sliders.

Users, upon discovering interesting patterns, need access to the actual data values. Drill down techniques may be used to obtain details about particular items. For example, when the user selects a glyph with the mouse, the data values for those items are displayed.

For intrusion datasets, one view is often not sufficient to answer all interesting questions. Many views, each answering separate, but related questions, may work together to provide insight. The views should be tightly linked so that operations in one view, such as color scale manipulations, propagate instantly to the other views. Together, the combination of several simple views is much more powerful than the sum of the individual views taken one at a time.

An effective user interface provides the user with constant and continuous feedback. However it is quite difficult to provide an instantaneous response to user commands with available standard IPC (interprocess communication) mechanisms, even on fast workstations. The requirement for near instantaneous response restricts the types of manipulations and the complexity of displays. As computer and networks become faster, these restrictions will become less onerous, but there will always be tension between visual detail and appropriate interaction techniques.

Aspects of intrusion detection visualization lend themselves well to traditional animation techniques. Animation, with each frame representing a single time period, is an ideal tool for analyzing large time-oriented datasets. For animation to be effective, the frames must transition smoothly and continuously. Large unexpected changes are jarring and stand out perceptually.

3. Haptic Visualization

Recent advances in computer interface technology now permit us to touch and manipulate conceptual computer-generated objects in a way that evokes a compelling sense of tactile reality [9]. This tactile interface, termed “haptics”, has been used for years by researchers in human psychophysics who study how people use their hands to sense and manipulate objects. What they have learned is basically that haptics rely on an action to stimulate perception. For example, to sense the shape of a cup, we do not take a simple tactile snapshot and go away to think of what we felt, rather, we grasp and manipulate the object in order to build a mental image of the cup. This co-dependence between sensing and manipulation is at the heart of understanding how humans can so deftly interact with the physical world [9]. The possibility to touch data, manipulate it, feel the pressure and resistance, preventing the user to move to restricted areas, and navigating him in 3D space might help to more efficiently perceive properties of the data [10]. Besides a sense of touch, haptic interfaces also provide a sense of force. According to [11], the sensing of forces is closely coupled to both the visual system and one’s sense of three-dimensional space.

Haptic interaction has been successfully applied to simulate specific tasks in several application areas [6]. Some of these areas include molecular docking studies, nanomanipulators for scanning tunneling microscope, and the simulation of knee palpation. From these applications it is evident that the use of a force feedback device during visualization is a natural output method for interactively conveying complex information to the user.

There are two basic approaches to interfacing haptics with visualization. The first approach deals with tightly coupling the visualization and the force field. The scene is rendered from the same data as the force field. The second approach deals with loosely coupling the visualization and the force field. The forces generated do not approximate a realistic feel of a virtual object, but rather convey meaningful structural information for data exploration purposes. Haptic data can come in a variety of forms, surface (Connolly surface), magnetism, viscosity, etc. A perception of touching a surface at a point is actually a perception of a resistance (or force) in a direction normal to the surface at that point. Therefore an illusion of a surface in a virtual environment can be created by a force which is normal to the surface at all points [10]. For loose coupling, it is possible to associate the haptic data with energy. The relation to energy allows one to map a lot of quantities to mechanical forces. In traditional physics, an integration of a force along a path equals to work and vice versa. The force is proportional to a gradient of the energy. Therefore, mapping certain quantities to force is fairly intuitive.

Typically lengthy computations for graphics or simulation require a decoupling of the haptic servo loop from the main application loop if high-quality forces are to be produced [11]. Such decoupling is even more critical for force display, where update rates of several hundred Hz are required to produce high-quality forces. A haptic display differs from graphical displays in several ways. The most significant difference is that the display and

graphics loops of virtual environments must be run asynchronously at approximately 20 HZ in order to maintain reasonable continuity and fluidity. With a slightly higher refresh rate one can achieve much smoother movement, but there is no reason to increase the number of frames past the limitations of visual perception.

4. Network intrusion visualization application

The system diagram of the network intrusion visualization application is displayed in Figure 1. The system begins with input from one or more network intrusion detectors. The output of the intrusion detectors may be of a simple ASCII or database format. The detection list is parsed and processed based on the currently selected model. A node placement list is then generated, indicating the location of each node in three-dimensional space (with the exception of the two-dimensional circular histogram model). From this list, a node-link map, composed of glyphs and links is created. The final scene is then rendered in one or multiple displays depending on the user's selection. The user is capable of manipulating several aspects of both the display and the data by way of the user interface. Besides basic input mechanisms such as the mouse and keyboard, the application supports both input and output from/to the PHANToM, a haptic device from Sensable Technologies. Coordinate values are read from the PHANToM to manipulate the camera location in the scene, and haptic forces are sent to the PHANToM depending on the force simulation model selected by the user.

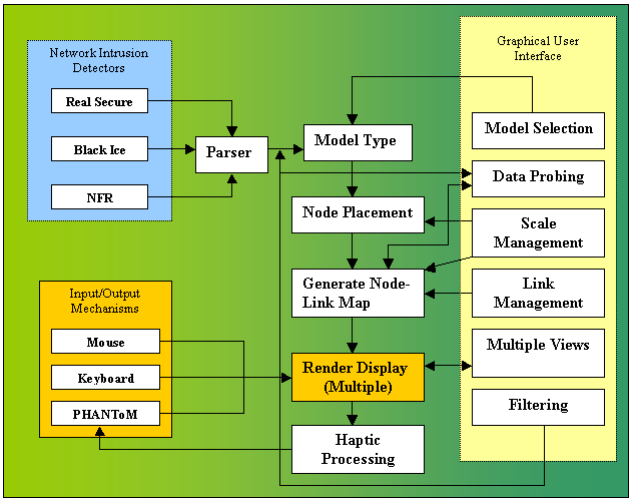

Figure 1: NIVA System Diagram

Through an OpenGL renderer, the application is able to allow the user to manipulate the graphics at a rate that varies approximately between 20 Hz and 50 Hz depending on the size of the data being visualized. While these rates are good for visual interaction, it is necessary to provide the servo loop of the haptic interface with a refresh rate of about 1 kHz in order to provide smooth and natural haptic feedback. To accomplish this, it is necessary to create two distinct processes. The first process, termed the rendering process, is responsible for reading the input data and rendering models depending on user selection. The second process, termed the haptic process, receives the rendered scene from the first process and applies camera manipulation based on the mouse and PHANToM device. In addition, this process also generates and applies the force vectors based on the current model selected by the user. These two independent processes communicate by way of system sockets.

Figure 2 shows a typical NIVA session. The first window in the Figure (the topmost window titled scene) is the rendering window for NIVA, which is currently displaying approximately one month's worth of attack information on a relatively large-scale network. The current model selected for this view is the IP Space model, in which each system in the attack database is mapped to a coordinate in three-dimensional space based on the value of three selected IP segments. The fourth segment is represented by the color of the glyph. The link color represents the severity of the attack. The second window is the graphical user interface, which allows the user to interact with the detection datasets in real time while performing the functions specified in Figure 1. The third and fourth window shows the output of Black Ice and Real Secure, which are commercial network intrusion detectors, respectively for the dataset under test.

In Figure 2, the application has isolated one destination system that is being attacked by multiple sources, which is then placed as the focus of the scene. The system supports full interactivity by the user, allowing the user to easily discover not only immediate threats, but also developing trends which occur over both space and time. For example, by examining the scene in Figure 2, several observations can be quickly made:

1. The most obvious observation is that this particular system has been under a considerable amount of attack in relatively short time span.
2. A majority of the attacking systems share the same domain (the first IP segment has been mapped to the glyph color), however their attacks are not severe (a link color of yellow has been mapped to a moderate attack), and thus does not necessarily pose any immediate threats.
3. The attacking systems mentioned in (2) all seem to lie on the same "plane" which indicate similar spatial (IP space) location – these were systems wired to a single hub in a lab transmitting SNMP broadcasts (information retrieved by probing)

These simple observations listed above without the benefit of a dynamic, interactive display, illustrates the possibilities of this visualization system. Both Black Ice and Real Secure were able to show the same information, however it would have taken extensive time and resources to arrive at a similar conclusion using their native visualization capabilities.

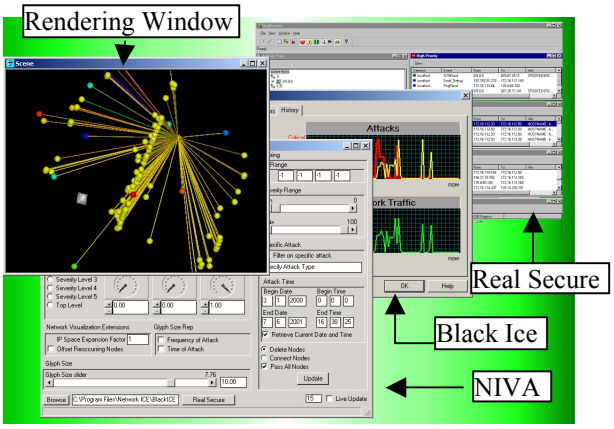

Figure 2. Typical NIVA Session

The gray diamond in the render window of Figure 2 is the location of the haptic device within the dataset. What this figure cannot show is that with the currently selected haptic model, the user could navigate within the dataset and detect that the systems that lie in the same plane seem to possess a strong attractive force, indicating that the systems launched attacks frequently. This potentially serious fact would have been overlooked with conventional visual displays.

4.1. Node placement algorithms

The IP-Space algorithm was the first node placement algorithm employed in NIVA, and represents the multidimensional scaling (MDS) statistical technique [12]. A common factor among the output generated by all intrusion detection systems is the Internet Protocol (IP) address of the source and destination computers. The IP address is composed of four segments, each of which provides information regarding the location of the computer on the global network. With the IP-Space algorithm, three of the four segments are mapped to the traditional three-dimensional Cartesian coordinate system in which a node is placed at the computer's relative location. The unused IP segment is usually assigned to represent the node's color or size. Lines representing attack relationships link certain nodes to one another. The properties of these lines provide further information concerning the attack properties. This model is not only easy to implement, but it permits the user to rearrange the display content to suit their needs and their forensic objectives.

NIVA also incorporates the "spring technique" as a node placement algorithm. With this technique nodes are positioned as though they are attached by springs of relative strength, each with an associated algorithm. We prefer individually associated algorithms, because it clusters strongly related nodes more compactly instead of filling space uniformly. The strength of connection is determined by both the nature of the attack and the frequency of the attack.

In Figure 3 another node placement algorithm called "the helix technique" is illustrated. With this technique nodes are strung along in a helix wrapped around a center node. This technique is suited for identifying multiple attacks to one system with some sort of sequential parameter. For example, Figure 3 represents the attacks occurring to one system at different times of the day. The nodes are placed along the helix according to the time of day the attack occurred. Several other parameters such as attack severity, system proximity (in IP Space) or even frequency of attack, may be mapped to node placement along the helix. Not only is this node placement algorithm visually appealing, when examined interactively, it allows the analyst quick and efficient access to the selected data, allowing attack patterns and relationships to be quickly discerned.

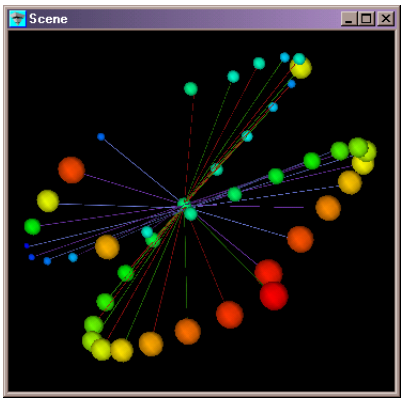

Figure 3. Helix Technique

When the helix model is viewed directly from above, it resembles a circle. Also if the connectivity lines were drawn outward instead of inward, the resulting model would resemble the solar plot model. This technique involves mapping some data parameter around the circumference of a circle producing a sort of circular histogram. With this technique, pattern recognition is greatly enhanced for a singular data parameter such as time of attack. Furthermore, this technique provides advanced automatic aggregation capabilities discussed later in this document.

4.2. Scale management

In order to effectively manage the scale of large networks, aggregation is heavily utilized within the application. Data aggregation simplifies large data sets by summarizing groups of data elements and representing such groups with a single graphical symbol or glyph [13]. Most of the node placement techniques used by the application incorporates automatic aggregation and deaggregation, which allows the greatest possible level of data detail to be shown. Aggregation is performed in two cases: a) if an object is occluded, or (b) if an object is too small to be perceived. Objects that fall into either of these two categories are aggregated with neighboring objects. A more intuitive form of data aggregation, sociograms [7] is integrated into the application. With sociograms, nodes of a similar nature are automatically aggregated. The user is provided complete flexibility in interpreting the exact meaning of "similar nature."

5. Haptic Interface

NIVA presents the user with several models of haptic interaction. Each of these models are designed to be used individually or in synchrony in order to provide the security analyst with an intuitive method of exploring properties of network intrusion data, which would prove inefficient using conventional visual or audio methods. Due to the nature of network intrusion data, it was not practical to model solid haptic surfaces (tight coupling). Rather loose coupling methods were utilized to represent the less tangible properties of the data.

5.1. Electric Field Haptic Simulation

Most of the visualization models in NIVA are based on link-node maps. By treating these nodes as particles possessing some charge quantity, it is possible to model forces within the dataset along the principles of electric fields. Since these fields do occur naturally in the physical world, the user can intuitively assimilate the information presented by the haptic device.

Coulomb stated that a force between two very small objects separated in a vacuum or free space by a distance, which is large compared to their size, is proportional to the charge on each and inversely proportional to the square of the distance between them [14]:

$$F = k\frac{Q_1 Q_2}{R^2} \quad (1)$$

where Q_1 and Q_2 are the positive or negative quantities of charge, R is the separation, and k is a proportionality constant. The proportionality constant k, can be written as

$$k = \frac{1}{4\pi\varepsilon_0}$$

The constant ε_0 is called the permittivity of free space and has the magnitude 8.854E-12 F/m. Thus, from equation (1), Coulomb's law is now

$$F = \frac{Q_1 Q_2}{4\pi\varepsilon_0 R^2} \quad (2)$$

The force quantity F given above is a scalar quantity. In order obtain the vector quantity needed for force haptic simulation, we need one more fact: the force acts along the line joining the two charges and is repulsive if the charges are alike in sign and attractive if they are of opposite sign. The vector form of Coulomb's law (2) can be written as:

$$\overline{F_2} = \frac{Q_1 Q_2}{4\pi\varepsilon_0 R_{12}^2} a_{12} \quad (3)$$

where a_{12} is a unit vector in the direction of R_{12} as illustrated in Figure 4.

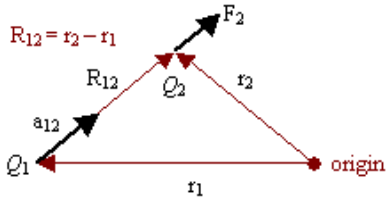

Figure 4. Vector force of Q2 (if Q2 and Q1 are of the same sign)

By representing (3) as a force per unit charge (and dispensing with some subscripts), the electric field may be written as:

$$\overline{E} = \frac{Q}{4\pi\varepsilon_0 R^2} a_R \quad (4)$$

Considering the case of a point charge distribution, the electric field may be written as:

$$\overline{E} = \sum_{m=1}^{n} \frac{Q_m}{4\pi\varepsilon_0 |r - r_m|^2} a_m \quad (5)$$

where n is the total number of point charges.

To apply this concept of electric fields to our network intrusion visualization with haptic integration, we have to map certain properties of network intrusion to that of electric fields. With NIVA, the user has the capability to select which parameters they wish to use in mapping the intrusion data to haptic feedback. The basic parameters used are attack type (numerical equivalent), attack severity, attack frequency, attack time, and system IP. It is also possible to map the results from the user configurable filters. These relationships may add invaluable information that could otherwise be difficult perceived visually. For example, a user has created a filter which ranks the frequency at which each system launched

attacks. This information is used to dynamically assign a charge quantity to each node in the rendering scene. As the pointer that represents the position of the haptic device moves within the rendering scene, the electric field intensity is calculated at its position using equation (5). The resulting vector force is applied to the haptic device, which provides the user with a sense of the frequency of attacks occurring within the varying "locations" in the dataset.

Expanding the subject of electric fields to streamlines, we realize that we can accurately model relationships among specific nodes with the haptic interface. From Hayt [14], the equation of a streamline is obtained by solving the differential equation $\frac{E_y}{E_x} = \frac{dy}{dx}$. By creating streamlines between nodes that have relevant relationships (determined by filters), the user may explore the haptic scene and actually discover these relationships by forces exerted on those streamlines.

5.2. Viscosity Haptic Simulation

Viscosity is an internal property of a fluid that offers resistance to flow. For example, pushing a spoon with a small force moves it easily through a bowl of water, but the same force moves mashed potatoes very slowly. This physical concept can be mapped to network intrusion visualization to indicate a wide range of properties. Once again, NIVA allows the user to select which properties are mapped to this physical phenomenon. For example, when moving through a rendered scene with a haptic device, the user may encounter a region of "space" where movement becomes stiffer (increase viscosity). This region could define properties such as increased attack severity or increased attack frequency.

The measurement of viscosity can be physically established by determining the velocity of a falling sphere. This is accomplished by dropping a sphere through a measured distance of fluid and measuring how long it takes to traverse the distance. Since the distance and time is known, the velocity, which is distance/time, can be calculated.

$$\eta = \frac{2(\Delta\rho)ga}{9v}, \text{ where}$$

η = viscosity
$\Delta\rho$ = difference in density between the sphere and the liquid
g = acceleration of gravity
a = radius of sphere
v = velocity = d/t = (distance sphere falls)/(time it takes to fall)

In the rendered scene, the empty space is assigned a particular density, which represents the liquid. At each point in the scene the imaginary ball is assigned a density and velocity, which depends on the selected property of the nodes closest to that point. The radius and gravity are kept constant. Consequently, each point in "space" is assigned a viscosity, which is relayed back to the haptic device.

5.3. Gravity Waves Haptic Simulation

According to Newton's Law of Gravity, two particles m1 and m2 a distance r apart attract each other with a force equal to

$$\overline{F} = \frac{Gm_1m_2}{r^2}\hat{r}$$

G is a proportionality constant called the Universal Gravitational Constant. Its value is 6.672 x 10^{-11} Nm^2/kg^2. The gravitational field is defined as the force per unit mass that is set up by a body of mass m. By assigning a mass to a particular node in the rendered scene, an associated gravitational field can be determined. If this field is set to pulsate (turn on and off) at a frequency that is inversely proportional to the proximity of the haptic pointer, which is assigned a much smaller mass, it is possible to draw the users attention, haptically, to the location of that node. This haptic simulation, termed "gravity waves", can be utilized as an unobtrusive means of providing significance to a single node or a group of nodes.

6. Experimental Procedure & Results

An experimental procedure was conducted to assertain the effectiveness of network intrusion visualization with haptic integration. Our goal was to assess whether haptics feedback would influence the speed or accuracy of the detection of specific attacks and the relationships within a network. Ten subjects were exposed to a network space: one with haptic feedback, and one without. The network space consisted of nodes and links similar to that of the IP-Space model.

The network space was populated with a combination of 85 instances of attacks. Each subject was asked to locate 9 specific attacks with certain relational information. The haptics group was also provided with information pertaining to interpreting the haptic feedback they would experience. In Figure 5, the time it takes for a subject to complete an experiment (in minutes) is displayed next to the accuracy of detection (percentage in half scale). The subject number is displayed on the x-axis and is segmented in two groups (subjects 1 – 5: visual only, subject 6 – 10: visual and haptics). From the plot, one can notice that even though there is only a small improvement in the speed of recoginition for the haptics group, there is a significant improvement in accuracy.

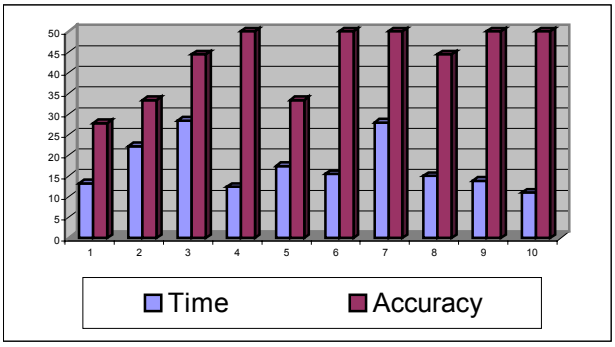

Figure 5. Haptics experimental results

7. Discussion

Network intrusion detection is a vital field of research in regards to mitigating the rising threat of malicious activity on today's networks. However the efficiency of network intrusion detectors is limited by their inability to effectively and concisely present the information relevant to the network analyst. Traditional two-dimensional displays and input devices suffer from issues dealing with clutter and insufficient interactivity capabilities. Therefore the integration of three-dimensional network visualization techniques with haptics is absolutely essential towards the analyst's ability to interact with the dataset and extract information relevant to his/her needs.

As stated before, NIVA is not a network intrusion detector. Rather, it is a haptic network intrusion visualization tool capable of representing data from several network intrusion detectors by a variety of different network visualization models and techniques in a highly interactive, multi-view system. By utilizing and combining key principles techniques of network information visualization with haptic technology, this system is able to augment the network analyst's ability to accurately understand malicious activity on a network. By allowing for multiple presentation formats and methods, the system exploits the human perceptual system to not only detect attacks on a system, but also patterns of attacks.

8. Conclusion

The research we have discussed in this paper is geared towards visualizing intrusions on small and large-scale networks through commercial network intrusion detectors. More than a tool for fanciful demonstrations, network intrusion visualization through NIVA can greatly improve the analyst's ability to detect and combat distributed attacks over large-scale networks. It is understood that malicious threats will increase in accordance with the expansion of information-rich communication networks such as the Internet. It is therefore essential to not only protect these vital networks but also possess the tools necessary to fully explore and understand the nature of the threats that exist on these networks. The capabilities we are developing will provide the tools necessary to accomplish these goals. Our direction of future research includes integrating more visualization and haptic models into the system as well as adding support for sound fields.

References

1. R. Becker, S. Eick and A. Wilks. *Visualizing Network data*, In IEEE Transactions on Visualization and Computer Graphics, vol 1,no. 1, March 1995
2. S. G. Eick, *Engineering Perceptually Effective Visualizations for Abstract Data*, In Scientific Visualization Overviews, Methodologies and Techniques, IEEE Computer Science Press, pp. 191-210, February 1997
3. K. C. Cox and S. G. Eick. 3D *displays of internet traffic*. In Information Visualization Symposium, Atlanta, Georgia, October 1995
4. K. C. Cox, S. G. Eick, and T. He. 3D *Geographic Network Displays*. Sigmod Record, 25(4):50--54, December 1996
5. S. Eick and G. Wills. *Navigating Large Networks with Hierarchies*, In Proceedings Visualization Conference '93, pp. 204-210, San Jose, Calif. ,October 19 93
6. R. Avila, Sobierajski, *A Haptic Interaction Method for Volume Visualization*. Proceedings of Visualization `96, Oct. 1996
7. M. Chalmers, and P. Chitson. *Bead: Exploration on information visualization*. Proceedings of the 15th Annual International ACM/SIGIR, 1992
8. M. Chuah, *Dynamic aggregation with circular visual designs*, Proceedings of the IEEE Symposium on Information Visualization, pp. 35 – 43, October 1998
9. K. Salisbury, *Haptics: The Technology of Touch*. HPCWire, Nov. 1995
10. A. Krenek, M. Cernohorsky, Z. Kabelac, *Haptics Visualization of Molecular Model*. Proceedings of WSCG '99, Feb. 1999
11. W. Mark, S. Randolph, M. Finch, J. Verth and R. Taylor II, *Adding Force Feedback to Graphics Systems: Issues and Solutions*. Proceedings of *SIGGRAPH '96*, pp. 447-452, August 1996
12. J. McHugh, A. Christie, and J Allen, *Defending Yourself: The Role of Intrusion Detection Systems*. IEEE Software, pp. 42-5, September/October 2000
13. M. Lehtinen, *Intrusion Detection: Managing the Risk of Connectivity*. IT Professional, vol. 1, no. 6, pp. 11-13, November/December 1999
14. W. Hayt Jr., "Engineering Electromagnetics", McGraw-Hill, NY 1989