A Novel Visualization Method for Detecting DDoS Network Attacks

Jiawan Zhang [1], Guoqiang Yang [1], Liangfu Lu [2,*], Mao Lin Huang [3],
1. School of Computer Science and Technology, Tianjin University, Tianjin , P.R.China;
2. Mathematics Department, Tianjin University, Tianjin, P.R.China, 300072;
3. Faculty of information Technology, University of Technology, Sydney, Australia
*Corresponding Author E-mail: liangfulv@gmail.com

Abstract. With the rapid growth of networks in size and complexity, netwok administrators today are facing more and more challenges for protecting their networked computers and other devices from all kinds of attacks. Unlike the traditional methods of analyzing textual log data, a visual interactive system called DDoSViewer is proposed in this paper for detecting DDoS kind of network attacks. DDoSViewer is specifically designed for detecting DDoS attacks through the analysis of visual patterns. We will discuss the data sources, visual structures and interactive functions that are used in the proposed visualization system. We will also discuss the advantages and disadvantages of the existing visual solutions for DDoS detection. The extraction and analysis of network data, the calculation and display of graphic elements' attributes and the pre-characteristics of DDoS attacks are all included in the new visualization technique. The experiments showed that the new system can detect DDoS attacks effectively.

Keywords: network security; DDoS attacks; information visualization; port scan

1 Introduction

Networks and data communication systems are becoming more and more complex [1]. However, there is no absolute solution to secure a networked system perfectly. Most existing network security techniques and tools still rely heavily on human detection of intrusions. These techniques require users to analyze and detect the anomalies and intrusions manually. To enhance the human perception and understanding of all kinds of network intrusion and attacks, network visualization has become a hot research field in recent years that attempts to speed up the intrusion detection process through the visual analytics. Unlike the traditional methods of analyzing textual log data, visualization can increase the efficiency and effectiveness of network intrusion detection significantly. It can not only help analysts to deal with the large-volume of analytical network data effectively, but also help network administrators to detect anomalies through the pattern recognition in visual graphs. It can even be used for discovering new types of attacks and forecasting the trend of unexpected events.

Some visualization techniques and tools have been proposed recently for detecting hostile attacks [2,3,4]. However, these techniques are more focusing on how to produce novel visual structures for general real-time monitoring of large volume of network traffic data, and they are not specifically designed for detecting DDoS (Distributed Denial of Service) attacks. Up to now there are no specific tools available for DDoS attack detection.

This paper proposes a novel visualization system called DDoSViewer that uses a new visual representation to display the main features and characteristics of DDoS attack. The proposed technique utilizes a variety of visual elements to map a collection of datagram to the graph for emphasizing DDoS patterns. The focus+context viewing and interaction techniques used in our system will also be discussed. The experiments have shown that the new system is able to detect port scans and many other kinds of DDoS attacks quickly and effectively.

The rest of the paper is organized as follows. Section 2 presents some of the related work. We describe our approach in section 3, including the details of data collection and processing, nodes coordinates calculation and their visualization. Case studies are shown in section 4. Finally, we give the conclusions and future work in section 5.

2 Related work

The study of DDoS attack detection has been popular for the last decade. Some works have been done in finding ways to detect DDoS attacks in large-volume alerts produced detection tools which employed visualization methods. Pearlman [5] proposed a new visualization in 2007 for network security by approaching the problem from a service-oriented perspective. This research provides a real time system for network administrators to monitor service activities, enabling for the early stage detection of attacks, including Denial of Service (DoS) attacks. Chris Lee etc [6] proposed a VisualFirewall in 2005 that seeks to aid in the configuration of firewalls and monitoring of networks by providing four simultaneous views that display varying levels of detail and time-scales as well as correctly visualizing firewall reactions to individual packets. Christos etc [7] introduced 3D interactive auto-stereoscopic (AS) displays for visual representations of attacks.

Although the above visualization techniques can assist network analysts in analyzing abnormal (or unusual) patterns of network data in the early stage of network intrusion detection, they can only produce alarms and in most cases the accuracy rate of alarming for real attacks is very low. Therefore, the actual identifications and classifications of a variety of attacks are still relied on human brain. Furthermore, so far there is no specific tools developed for detecting DDoS attacks, and the above approaches are only focusing on the visualization of suspicious network activities and they do not help in the analysis of network event characteristics.

In this work, we focused on both the analysis of DDoS features and the investigation of novel visual representations. This enables the new system work effectively in some complex situations for DDoS attack detections, such as Smurf attacks detection, port scans detection etc.

3 Our new approach: DDoSViewer

Network Visualization (NV) is a part of the information visualization. The main steps involved in NV are 1) data collection and pre-process, 2) visual mapping, and 3) graphics generation. we will discuss these three steps with the details in the design stage.

3.1 Data collection and pre-process

The current network security requires information visualization to be able to display sufficient network information with a meaningful visual format, and efficiency in visual processing. The multiple-dimensional visualization of raw network data is one of such meaningful visual format that attracted many researches working on it for several years. In multi-dimensional visualization, the dimension reduction technique is essential to be considered first, and then the format of the data including source IP, destination IP, destination port, packet size and time-stamp can be obtained accordingly.

To analyze the raw data, a hash-table is used for data storage, and the keywords are expressed by the strings, which includes three parts: *source IP*, *port numbers* and *time-stamps* which are chosen by user to set the time interval $\mathcal{K}$. Any difference of the three parts in the new element will be inserted into the hash-table, and will be rendered as a new node, which expresses the relationship between the two hosts. The value of $\mathcal{K}$ denotes the total amount of data transmitted between two linked nodes. After having selected a time interval $\mathcal{K}$ in the interface (default value as the beginning of the programming), $\mathcal{K}$ will be introduced into the statistical module. Statistical module uses the window that built by the scale of $\mathcal{K}$ processing the data from the beginning of the raw data to the end. The data which included in the scale of $\mathcal{K}$ will be processed and the others will not.

3.2 Drawing of Nodes

The key to the visualization is drawing of the nodes for showing the present network status. Thus, the calculation of the geometrical positioning of nodes is essential. In our work the principle of the nodes positioning is based on the geometrical distance and the communication frequency between the new node and the center node which have the same trend. That is, if a console node communicates with the central console node more frequently, it will be moved away from the central one more further. There are two core issues for better visualization:

1). Positioning a new node: Based on the communicated frequency, the liner distance between a Console Node n_c and the Central Console Node n_{cc} is calculated by the following model. First, we define some constants and valuables: F_{max} is the maximum communicated frequency, $F_{\min}$ is the minimum communicated frequency, and $R_{\max}$ is the maximum radius of the available

screen space. R_{unit} is a unit radius that is defined in formula (2), where d represents the greatest difference of the frequency defined in formula (1).

Suppose that F_n is the frequency value of a new console node n_c calculated from statisticas. R_n is the radius of n_c, defined by formula (3). After we get the radius, we can calculate the geometrical position of n_c, $D(n_c)=(x, y)$ using formula (4).

In Fig. 1, the point O is the Center Console Node n_{cc}, and n_c is a new console node. The absolute value of the abscissa of the point X is in the range of $[-R_x, R_x]$. Using the formula (4) we can obtain the values, and then we can calculate y using (5).

$$d = F_{\max} - F_{\min} . \tag{1}$$

$$R_{unit} = \frac{R_{\max}}{d} . \tag{2}$$

$$R_x = F_x \times R_{unit} . \tag{3}$$

$$x = Random(\ ) \times R_x . \tag{4}$$

$$R_x = \sqrt{(x - x_0)^2 + (y - y_0)^2} \rightarrow y = \pm\sqrt{R_x^{\,2} - (x - x_0)^2} + y_0 . \tag{5}$$

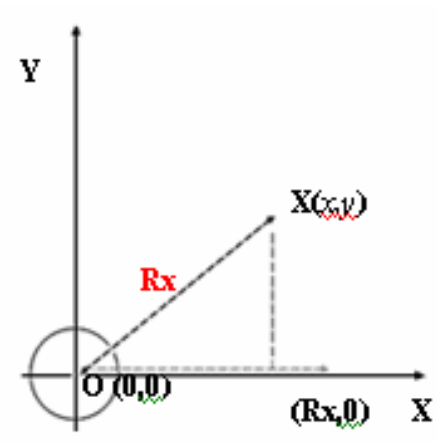


Fig: 1. Node positioning

2) Node overlapping problem: If some nodes are overlapped in the visualization, then the main graphic attributes of nodes may not be completely displayed. For example, the attributes of the line between console nodes and the colors of the console nodes may be hidden when node overlap occurs. In our visualization, we addressed

this problem with an effective and simple method. When a new node is to be generated, the visualization will search all the existing positions of displayed nodes. If there is a node overlap found, the system will then re-generate a new *X* coordinate, and a new *Y* coordinate for the new node. However, this problem cannot be completely solved. Although the scope of the *X, Y* coordinates is sequential and unlimited, we still can not obtain a clear view with no node overlaps if the number of nodes to be displayed in the same radius becomes large. Considering the arc length with the same radius is always limited, and the size of the node can't be modified. The technique of "magnifier" can be used to solve this problem by adjusting R_{unit} defined in the formula (2) manually. It can be enlarged in the local view through adjusting the parameters to achieve amplification. This will be discussed in the next section.

3.3 Graphic Design of Nodes

After the positioning of nodes,, the information of the geometrical location of nodes (date items) will be stored in the program, and then the nodes will be drawn graphically through the graphic design module, which is depends on the domain characteristics of nodes. The graphic design model can be described below:

The networking connection between a node n_c and n_{cc} can be described by several domain specific attributes and the value of these attributes can be measured in a certain time interval $\mathcal{K}$. In our graphic design, we attempted to map the domain specific attribute (the networking attributes) into the graphical attributes (the coloring scheme). For example, we may use the "red" color to represent the high value of a certain networking attribute. In our graphic model, a console node n_c is consisting of a range of concentric circles, and the number of ports involved in the networking connection is represented by the color contrast grade.

Each node is displayed as a range of concentric circles (see Fig 2) which have equal width between each pair of circles, C_i and C_{i+1}. Each circle displays one color in a N-level color scheme (see Fig 2). The color of the consecutive circle is mapped the consecutive color ribbon. At the same time the width *P* express the distance between the consecutive colors. The width *P* is determined by the number of the ports connected between nodes n_c and n_{cc}. If the connection is based on many ports, the span between colors would be very larger and the nodes' color contrast grade would be stronger. Oppositely, the span could be smaller and its color trends to be a single color. All of these are shown in Fig. 2[13]

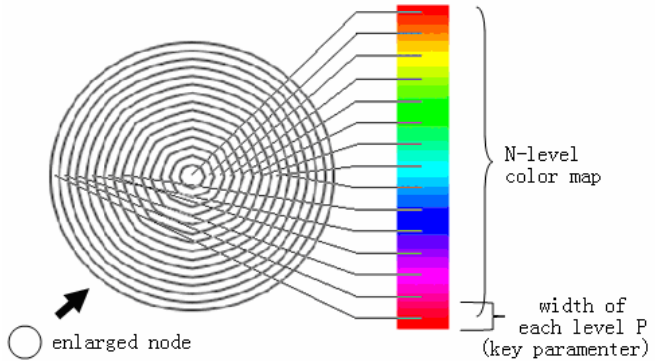


Fig. 2: The color scheme in node design

For detecting different abnormities and identifying different types of attacks, we need to utilize different value of the parameters. Therefore the adjustment of the parameter is critical to the system. The characteristics of DDoS attack are best to be presented by multidimensional and large scale visualizations. However the limit of the display space is a problem. Therefore, the interactive zooming technique is crucial for users to have both the global view of the nodes interaction and the detail view of a node that can help in identifying the type of attacks. In this model, the user can adjust the value of parameters in the system to catch the optimized view for detecting abnormal actions. For example, the user can manually adjust the length of radius and the time intervals *K* in the real-time raw data to catch the most distinctive features of DDoS attacks.

4 Case studies

In this section we describe several examples of using DDoSViewer for visual analysis and detection of DDoS attacks. One remarkable characteristic of DDoS attacks can be described as that in a short time the attacked host receives a lot of date packets sending from a large number of strange IP addresses. For example, the characteristic of Smurf attack is that in a short time one host may communicate with large number of IP addresses simultaneously and most of the source IP addresses have never appeared in the current host before. The experimental data we used are caught from LNA in the Image and Graphics Institute, Tianjin University.

By using DDoSViewer, DDoS attacks can be detected very easily. In Fig. 3, there are three isolated nodes around the center host. The interactive technique allows the exploration of detailed attributes of nodes easily. By having a close look of detailed data shown in Fig 3, we can easily find that these network connections are mainly related to port 23 and 80. Thus, the analysts may assume that these nodes may perform data transmission services, such as ftp transmissions (in port 23) or web transmissions (in port 80), and there is nothing abnormal. In comparison with other nodes, the line color between the third node and the center host is deeper (the red

color), and from Fig. 3, we can see that there are more data communications with port 43969 of one host. If we want to have a close look of this host, we can get its IP address 59.247.12.45.So it can be assumed that the user is using a file transfer service. We can also see that there are many nodes surrounding the center node in Fig. 3. After interactively exploring the detail of nodes, we discovered that all of the surrounding nodes have different IP addresses. All log data items are collected in the same time interval: $\mathcal{K}$=2. By looking over detailed information of these surrounding nodes, we also found that all the nodes are connecting with the port 7 of the center host at the same time: 2008-4-2 18:05:02. The sizes of the transmitted data between the surrounding nodes and the center host are very small. It could be just an Echo message, such as a returned message after the host receives a PING packet. Therefore, we can then identify this visual pattern shown in Fig 3 as a typical "Smurf" attack, which is quiet different from the other patterns we generated through DDoSViewer. In fact, our system can detect Smurf attacks that are not restricted to the Echo package. Rather the system could extend its pattern recognition capacity to identify other abnormalities (or attacks) based on the distinctive features of the visualization generated by DDoSViewer.

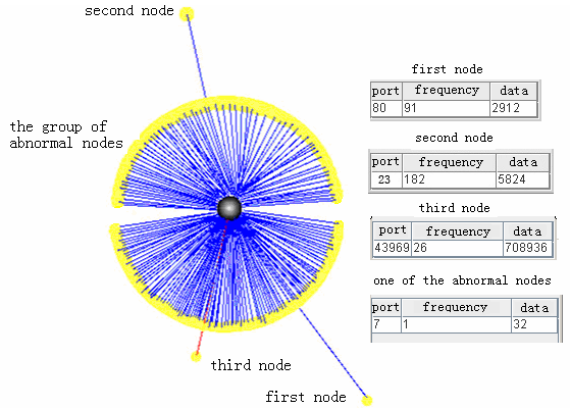


Fig. 3: A distinctive pattern of Smurf attack: many nodes surrounding the host node with small data packages and stranger IP addresses.

Port-Scan is another preliminary type of DDoS attacks and we can also extract its main domain specific features and generate distinctive visual patterns for analysts to quickly detect it. In Fig. 4, we can see that there are two obvious abnormal nodes, the first node and the second node. In comparison with other nodes in visualization (for example nodes in group A), these nodes are far away from the center node. The main features of abnormal nodes are that they have more color levels than others and they also have a larger amount of networking traffic (data transmissions) with the center node. In Fig. 5, we can easily find that in each port of the abnormal nodes only transfer a very small data package, but the scanned ports received a large-volume of data, and the colors of the abnormal nodes are very complicated. We believe that the distinctive visual pattern generated as shown in Fig 4 is clear enough for network analysts to easily and quickly identifying the port-scan attackers.

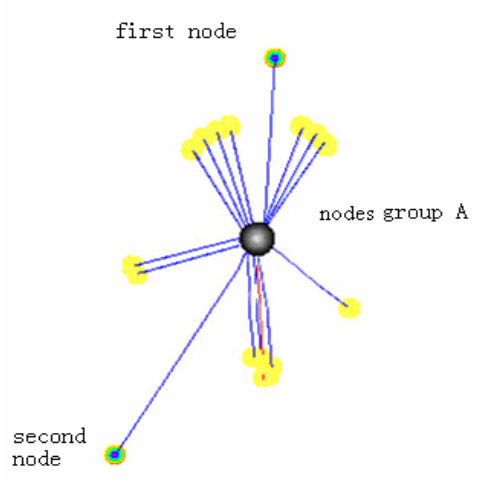
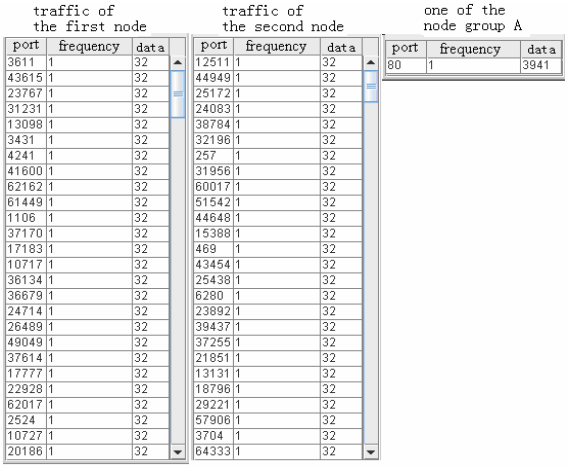


Fig. 4: A distinctive pattern of port-scan attack.



port	frequency	data
3611	1	32
43615	1	32
23767	1	32
31231	1	32
13098	1	32
3431	1	32
4241	1	32
41600	1	32
62162	1	32
61449	1	32
1106	1	32
37170	1	32
17183	1	32
10717	1	32
36134	1	32
36679	1	32
24714	1	32
26489	1	32
49049	1	32
37614	1	32
17777	1	32
22928	1	32
62017	1	32
2524	1	32
10727	1	32
20186	1	32

port	frequency	data
12511	1	32
44949	1	32
25172	1	32
24083	1	32
38784	1	32
32196	1	32
257	1	32
31956	1	32
60017	1	32
51542	1	32
44648	1	32
15388	1	32
469	1	32
43454	1	32
25438	1	32
6280	1	32
23892	1	32
39437	1	32
37255	1	32
21851	1	32
13131	1	32
18796	1	32
29221	1	32
57906	1	32
3704	1	32
64333	1	32

port	frequency	data
80	1	3941

Fig. 5: the detail information of nodes displayed in Fig 4.

5 Conclusion and future work

This paper proposed a new visualization method called DDoSViewer that focuses on creating of distinctive visual patterns for analysts to effectively and efficiently detect DDoS attacks, such as the Smurf attacks and port-scan attacks. The new system is working mainly based on the statistics model of the time-stamp, rather than the

traditional packets analysis model. Interaction techniques with multiple-views are used to display both the overall view of the linkage attributes and the detailed view of node attributes, which are represented by geometrical attributes and rich graphic properties, such as colors and the locality of nodes.. The experiments have shown that the pattern of the attacks can be distinctively generated in DDoSViewer and these distinctive patterns could significantly assist the analysts in detecting DDoS attacks. In the future, we plan to draw the graphics in 3D visual spaces, and set up more visualization functions to improve the representations of nodes that could increase the accuracy of network attack detections.

Acknowledgments: This work has been supported by National Natural Science Foundation of China under Grant No.60673196； the Natural Science Foundation of Tianjin, P.R. of China, under Grant No. 07F2030.

References

1. X. Yin, W. Yurcik,: et al. “VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness.”, Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, Washington, DC, USA, ACM Press.
2. Robert F. Erbacher.: “Visual traffic monitoring and evaluation”, In Proceedings of the Conference on Internet Performance and Control of Network Systems II, 2001, pp 153–160.
3. L. Girardin and D. Brodbeck.: “A visual approach for monitoring logs”, In Proceedings of the 12th Usenix System Administration conference, 1998, pp 299–308.
4. Chris Muelder, Kwan-Liu Ma and Tony Bartoletti,: “A Visualization Methodology for Characterization of Network Scans”, Visualization for Computer Security, 2005, pp.29-38
5. J. Pearlman, P.R.: “Visualizing Network Security Events Using Compound Glyphs from a Service-Oriented Perspective”, In Visualization for Computer Security. VizSEC 2007: Proceedings of the Workshop on Visualization for Computer Security, 2007, pp. 131~146.
6. Chris P. Lee, J.T., Nicholas Gibbs,Raheem Beyah,John A. Copeland.: Visual Firewall: Real-time Network Security Monitor. in IEEE Workshop on Visualization for Computer Security 2005 (VizSEC 05), 2005:129~136.
7. Christos Papadopoulos, C.K., Alexander Sawchuk, Xinming He, “CyberSeer: 3D Audio-Visual Immersion for Network Security and Management.”, Proceedings 2004 ACM Workshop on Visualization and Data Mining for Computer Security. 2004. Washington, DC, USA: ACM Press,pp: 90~98.
8. A. Hussain, J.H.a.C.P.: A Framework for Classifying Denial of Service Attacks. in Sigcomm 2003. Karlsruhe, Germany. 2003: 99~110.
9. Muelder, C., Ma, K.L., Bartoletti, T.: A visualization methodology for characterization of network scans. Visualization for Computer Security, IEEE Workshops, 2005, pp. 4 – 4.
10. Conti, G., Abdullah, K.: “Passive visual fingerprinting of network attack tools”. VizSEC/DMSEC ’ 04: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, 2004,pp. 45 – 54
11. Jonathan McPherson, Kwan-Liu Ma, Paul Krystosk, Tony Bartoletti, Marvin Christensen.: Portvis: “A tool for port-based detection of security events”. In: ACM VizSEC 2004 Workshop, 2004, pp. 73 – 81
12. Pin Ren, Yan Gao and Zhichun Li,: “IDGraphs: Intrusion Detection and Analysis Using Histographs”, Visualization for Computer Security, 2005, pp.39-46

13. Stuart K. Card, Jock D. Mackinlay and Ben Shneiderman,: “Readings in information visualization: using vision to think”, Morgan Kaufmann Publishers, 1999
14. Rawiroj Robert Kasemsri,: “A Survey, Taxonomy, and Analysis of Network Security Visualization Techniques”：[Master Paper], USA, Georgia State University, 2005
15. Richard A. Becker, Stephen G. Eick, and Allan R.Wilks, “Visualizing network data”. IEEE Transactions on Visualization and ComputerGraphics,1995 1(1):pp.16–28.
16. Prefuse, http://www.prefuse.org/
17. Mukosaka, S.;,Koike, H.:“Integrated visualization system for monitoring security in large-scale local area network Visualization”,APVIS '.2007 6th International Asia-Pacific Symposium, 2007,pp.41– 44
18. Musa, Shahrulniza, Parish,etc.: “Visualizing Communication Network Security Attacks”, Information Visualization,IV '07. 11th Internati onal Conference, 2007, pp. 726-733
19. Pavel Minarik1 , Tomas Dymacek.: “NetFlow Data Visualization Based on Graphs”, In Visualization for Computer Security ,VizSEC 2008: Proceedings of the Workshop on Visualization for Computer Security, 2008, pp. 144-151