Research on Network Security Visualization Based on Graph Database

Ye WANG*

The 28th Research Institute of CETC, Nanjing, 210000, China
*Corresponding author

Keywords: Network security, Visualization, Graph database.

Abstract. The combination of network security technology and data visualization has formed a new hot research direction - network security visualization. In this paper, network security visualization framework based web is proposed firstly, and then the composition of the framework and the main functions of its constituent elements is introduced. Secondly, based on the analysis of network security data structure, a network security data organization method based on graph database is proposed. Finally, based on the above method, a network security visualization prototype system is implemented. The results show that the two types of views of the system show network security situation from different dimensions, and it is feasible and effective to analyze network security data.

Introduction

With the rapid development of information technology, computers and networks have become more widely used in military, politics, finance, industry, commerce, and people’s life and work. The continuously expanding scope and evolving content of network security threats have increased the pressure on network security, and it also brings new challenges to network security. Therefore, in the face of large and complex data, how to efficiently analyze the internal structure and the connections, and master network security situation has become an important issue in the field of network security.

Traditional analysis methods have a series of problems such as excessive cognitive burden, weak interaction, inability to predict and defend network security events in advance in analyzing massive data. Network security visualization can present abstract networks and data in the form of graphic images, help network security analysts analyze network conditions, identify network anomalies and intrusions, predict the development trend of network security events, and provide strong support to discover the rules and potential security threats[1].

Since 2014, IEEE has held a seminar on network security visualization every year (VizSec)[2], marking the formal establishment of this research area. From 2011 to 2013, the Visual Analytics Challenge Competition organized by IEEE VIS[3] has adopted network security data as a competition topic, which has pushed the field to a new research boom. In 2016, the Visual Network Security Technology Forum was held to gather experts from many authoritative academic institutions to discuss forward-looking technical viewpoints of visual network security[4].

In this paper, according to the characteristics of network security visualization system, a web-based network security visualization framework is proposed. Based on the analysis of network security data structure, a network security data organization method based on graph database is proposed. And multiple views are used to represent the network security data, which can provide support for network attack trend prediction and network security precautions.

Web-based Network Security Visualization Framework

Framework Architecture

The web-based network security visualization framework is shown in Figure 1. It is divided into client and server. Client provides users with the network security visual interface and interaction control
function. Server deals with the requests submitted by the client, implements data access, data processing, data analysis, and access to map data through the map server.

Figure 1. The web-based network security visualization framework.

The data processing flow of the framework is as follows:

Step 1: The client submits a request to the web server in order to obtain customized web security data or map data;

Step 2: After receiving the client’s request, the web server parses the request, and according to the request type calls the corresponding services for data access, processing, and analysis; if it requests the map data, it communicates with the map server through the map service proxy, and then the map server processes and accesses the geographic information database and returns the map data;

Step 3: The web server returns the generated data, pictures, files and other results to the client.

Server-side Design

The server side includes a web server, a map server and a map service proxy. The web server is a core, providing the capabilities including data analysis, data processing, and data access interface.

Data access interface: According to the client request or the upper-level service, to provide add, delete, modify and query interfaces to the network security database, return the customized data.

Data processing: Combine, correlate, and merge the acquired raw data collected from various types of safety devices to complete preliminary processing.

Data analysis: Classify network security data according to different dimensions, evaluate security risk factors, and generate visualized data.

Client Design

The client visit the target site through a web browser to present the user with a web security visual interface and provides the user with an interaction control interface.

Visualization: The processed and analyzed network security data is displayed in multiple views, in multiple perspectives, and in multiple levels. The presentation methods include geographical view, network topology view, bar charts, pie charts, line charts, tables, dashboards, etc.

User interaction control: Provide view zoom, roaming, point selection, layer control, signage interaction, floating button interaction and other view interaction control interface.

Network Security Data Organization Method Based on Graph Database

Network Security Data Structure Analysis

The network security data mainly includes network traffic data, firewall data, intrusion detection system data, etc., and has the characteristics of large-scale, high-dimensional, non-structured,
How to effectively organize and standardize network security data is an important issue for network security data analysis.

By analyzing the network traffic data, we can obtain the source IP address and the destination IP address of the data packet, so that the nodes in the network and the connection relationships between the nodes can be obtained. By analyzing the events detected by the firewall and intrusion detection system, we can obtain the source IP address and the destination IP address of the event. Therefore, whether it is network traffic data, firewall data, or intrusion detection system data, it involves two basic attributes, source address and destination address.

Therefore, in this paper we abstract the network security visualization data into a structure composed of points and edges. Based on the physical elements of the communication network (network equipment, computing equipment, etc.), and according to its connection relationship, the network security visualization base map is formed.

Using a relational database as the underlying storage requires constructing a query statement when associating query nodes with each other, which results in low query efficiency. In this paper, we uses the graph database[5] to realize the association query. Compared with the relational database, it uses the characteristics that the relationship between nodes is consistent with the graph database to map the nodes and relationships into a graph database structure, and converts the complex query analysis statements into relatively simple graph query statements which improves query efficiency.

**Graph Database**

The graph database model is a generic data structure that uses a directed graph to model and store data in graphs. The nodes and relations of the graph database model correspond to the vertices and edges of the normal graph, respectively. Nodes are organized by relationships, and a number of nodes and relationships can form complex graph models in certain directions. Nodes and relationships have multiple attributes. Each different type of node or relationship is distinguished by a tag. A graph database can store several graph models.

In this paper, we uses the Neo4j map database[6], Neo4j is a high-performance NoSQL graphics database, with high availability, scalability and high performance. Neo4j, its graph model is relatively simple, including nodes and edges. Nodes are used to represent entities and have key-value pairs for multiple attributes. Key-value pairs are described in JSON format. Edges are used to connect one or more nodes in a certain direction into interconnected graphs. Relationships have directionality and key-value pairs for multiple attributes. There can be multiple different relationships between two nodes. The direction can be either unidirectional or bidirectional. The number of attributes can also be dynamically extended.

Figure 2 depicts a typical two nodes graph model. The label of the node is the same as the name of the entity. The label of the edge is consistent with the name of the relationship, and several attributes can be added as needed.

**Network Security Visualization**

Based on the research of network security visualization framework and network security data organization method based on graph database, in this paper, we designs and implements a network
security visualization prototype system, focusing on two main types of views: geographical view and network topology view.

**Geographical View**

The geographical view of the network security visualization system is shown in Figure 3(a). The geographical view is based on the geographical location information of each node, and shows each node and its attack situation on the map. Attacks are performed by moving the beam of light from the point of attack to the point of attacked and represent the severity of the event in different colors. Geographical view allows network security analysts to fully grasp the overall situation, so that timely response measures can be taken.

**Network Topology View**

The network topology view of the network security visualization system is shown in Figure 3(b). The network topology view uses the physical or logical connection relationship between nodes and nodes as a base map. It is based on force-oriented algorithm layout, supports layer overlay, provides domain shrinkage expansion capabilities, and represents application data such as business traffic and service status, as well as the process of attack and defense events. Based on the network topology view, network security analysts can more clearly analyze and identify network attack paths.

![Network security visualization](image)

(a)The geographical view  (b)The network topology view

Figure 3. Network security visualization.

**Conclusion**

The network security visualization technology presents high-dimensional and abstract data in an intuitive graphic format to help network security analysts analyze network security situation. In this paper, a web-based network security visualization framework is proposed. Based on the analysis of network security data structures, a network security data organization method based on graph database is proposed. Finally, a network security visualization prototype system is implemented, which can provide support for network attack trend prediction and network security precautions.

**References**


