Presenting Scattered Data & Flow Data in efficient way

1. Introduction of Cyberthreat real-time Map

Cyberthreat real-time Map(https://cybermap.kaspersky.com/) is a Web-based map application developed by Kaspersky Lab. It aims at detecting global cyberthreat in real time. There are two types of data: scattered data (OAS①, KAS②, ODS③, MAV④,VUL⑤) and flow data (VUL⑥, IDS⑦, WAV⑧) used in the final visualization work. All data can be searched in both plane and sphere views.

2. Scattered Data

In Cyberthreat real-time Map, scattered data is created when cyberthreat occurred. Visualizing them helps users sense the distribution of multitype of Cyberthreat. Here, the idea of Dot map is the foundation of scattered data visualization techniques. Hence, Map developers designed dynamic map symbols to vivid final Map presentation.

2.1 Dot Map

Dot Map using equal-sized and attributed dots to picture a quantity or phenomenon in given area [1]. According to the type of dot, Dot Map is classified into dot density map and dot distribution map. In our review case, the map (Figure 1) is based on dot distribution map whose point symbol only records if event occurs at certain location. For dot density map, each point symbol valued by fixed round number. Unlike the dot distribution map, the place of dot doesn't present real location, it can always be the centroid of area unit [2].

Figure 1: Distribution of ODS

2.2 Dynamic Map Symbols

Wu Xiangfang et al. summarized the data structure for dynamic symbol (Figure 2) [3]. According to this structure, Take ODS as an example, there are three main parts exist in its dynamic symbol. 1. Animation style: Jump. When the cyberthreat attacks at certain

location, the point symbol would jump out. It helps to aggregate the phenomenon's change 2. Visual parameter: Color and Brightness. Different color of the symbol presents different type of data. By adding the brightness of the color, cluster center would be more obvious. 3. Rhythm: symbol size changes with time. The point symbol is based on hexagon. along the Z axis of symbol, the size of the hexagon changes with time. It prevents the crowded of symbols.

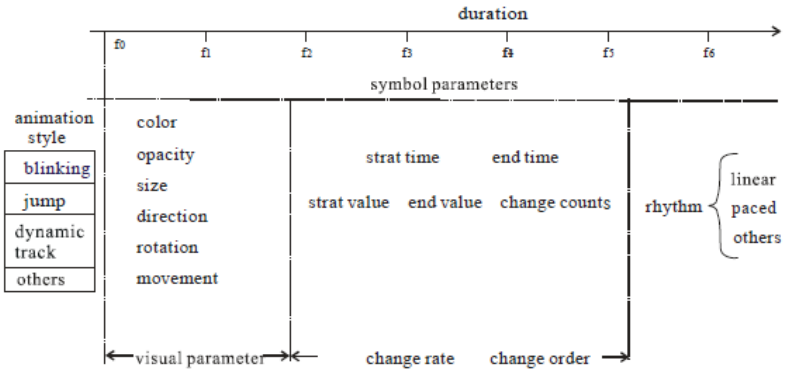

Figure 2: Data structure of Dynamic Symbol

Figure 3: Dynamic symbol for ODS

2.3 Data in Plane or Sphere

Developers also implemented planE (Figure 1) and sphere views (Figure 5) to present data together.

Figure 5: Sphere view for ODS

In plan view, it is clearer about the data distribution and clusters pattern than sphere view. But it would cause distortion problem which could be solved using global. At the same time, by rotating the global, it is more convenient for users to focus on their interesting location than in plan view.

2.4 Analyzation

Map for scattered data in Cyberthreat website obtains both advantages and disadvantages from dot map. Dynamic symbol helps to detect distribution change in real time more clearly. It is easy for users to see how phenomenon distributed and capture the point clusters on the map.

3. Flow Data

Flow data usually contain the start and end location (usually geographic) where objects or phenomena occur as well as their start-time and end-time as attribute data. In Cyberthreat real-time map, like the Kaspersky real-time map being reviewed, locations of where DDOS, Malware or other cyber-attacks are known and the time of the attacks. Visualizing such phenomena on an interactive map helps users understand what is going on, where and when. The data flow visualization technique used in this map in review utilizes animation also.

3.1 Flow Map

A Flow map is a mix of maps and flow charts which show movement of objects or phenomena from one location to another. This includes the number of people in a migration, the number of packets in a network, or the flow of currency from one country to another. [4] Sometimes, flow maps also indicates the volume/amount of the object or phenomenon.

Figure 6. Flow map visualization in planar view

3.2 Dynamic Map Symbols

Still in reference to Wu Xiangfang et al. research on dynamic symbols summarized the data structure for dynamic symbol (Figure 2) [3]. For instance, WAV (Web Anti-Virus) data utilizes three categories in its dynamic symbolization. For animation, dynamic tracking is used. This technique tells of the start and end locations. In terms of visual parameters, it makes use of size and color. The size difference shows the data volume while the color helps in in selective visualization. And for direction, the start and end time data is used.

3.3 Data in Plane or Sphere

The below figure is the flow map in a globe. The dynamic symbol alongside animation vividly shows the movement of data from one part of the globe to the other.

Figure 7. Flow map in globe view

3.4 Analysis

For every map technique selected by a map maker, designer or developer, there are certain pros and cons. Flow maps as executed on this site in preview, gives users a good understanding of how real-time data flow can be easily visualized. Subsequently, it gives an excellent aggregate understanding of regions with the most activities. However, because arrow heads are not used, users would be required to pay rapt attention to figure out where the flow originates and where its destination is.

4. Summary

Overall, the interactive map is very informative and could be used in making quick decisions. Its excellent choice of design techniques to represent the large amount of data being collected is efficient.

5. Reference

[1] https://gisgeography.com/dot-distribution-graduated-symbols-proportional-symbol-maps/. Accessed on 10 January, 2019

[2] https://en.wikipedia.org/wiki/Dot_distribution_map Accessed on 10 January, 2019

[3] Xiaofang W, Qingyun D, Zhiyong X, et al. Research and design of dynamic symbol in GIS[C]//Proceedings of the International Symposium on Spatio-temporal Modeling, Spatial Reasoning, Analysis, Data Mining and Data fusion. 2005.

[4] https://en.wikipedia.org/wiki/Flow_map Accessed on 10 January, 2019.