Application of Schneiderman's Mantra to Identify Malicious Behavior in Network Graphs

Nicholas Spyrison[*] Miji Kim[†] Ha Nam Anh Pham[‡]

Monash University, Faculty of Information Technology

Abstract

The VAST Challenge 2020 Mini-Challenge 1 involves network data. Specifically, there is a large multi-modal network synthetic dataset from which subsets of a template and 5 suspects must be compared and contrasted, akin to a police line-up of suspects. Our approach follows Shneiderman's mantra; namely 1) overview, 2) zoom-in, 3) details on demand. We capture an overview of the data with heatmap and network visualization across the different data channels. We zoom in by exploring the network visualization and t-SNE embedding of the suspect subgroups. Lastly, we look at single channels of data within the remaining suspect via highly customized animations across time.

Index Terms: Human-centered computing—Visualization—Visualization application domains—Information visualization Human-centered computing—Visualization—Visualization application domains—Visual analytics Human-centered computing—Visualization—Visualization techniques—Graph drawings

1 Introduction

VAST Challenge is an annual contest where teams compete to solve a series of tasks around a hypothetical scenario and related synthetic data. VAST 2020 mini-challenge 1 focuses on a hypothetical cyber-attack that caused widespread internet outages. In order to identify the culprits, a template network has been provided and verified by domain experts to be indicative of the malicious behavior that needs to be identified. 5 suspect networks of particular suspicion are included to compare and contrast with the template. Together, these 6 networks are relatively small selections of the full set of network interactions provided in the challenge for optional consumption or identification of other malicious networks.

2 Approach

Our approach follows Shneiderman's mantra for extracting information via data visualization (Shneiderman, 1996 [5]); namely, the structure of our paper and workflow followed overview, 2) zoom-in, 3) details on demand.

3 Application

3.1 Heatmap

To get a higher level picture of the distribution of observations across the data sources and transaction channels (also called edge names). From figure 1 we see that the distribution between sources is consistent. The demographic channel has the bulk of the observations while the co-authorship channel is not always used. We conclude that the suspect networks are of similar distribution to the template network and have context for the frequency of the different channels.

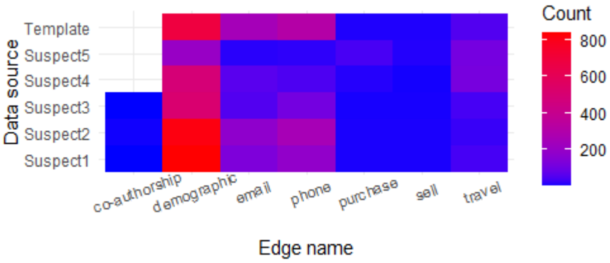

Figure 1: Count of observations within each data subset across the edge names. The bulk of the observations happens in the demographic channel. Co-authorship is not used in all networks. Distributions are similar between data sources.

3.2 Network

To identify and contrast specific features across different networks, network layouts were designed. As seen from figure 2, faceting techniques were applied within data sources and node names to better compare and contract each subset network. It is noticeable that compared to the suspects, the template network has a massive number of transactions moving toward the inside of the densest region. On the other hand, suspects 4 and 5 are having more outgoing data instead of incoming data. We conclude that suspects 1, 2, and 3 exhibits more similarities in the flow of transactions with the template network.

3.3 tSNE

T-distributed stochastic neighbor embedding (tSNE) is a non-linear dimensionality reduction technique purposed by van der Maaten, 2008 [6]. The application of nearest neighbors preserves local structure in the full dimensionality while distorting the global structure to fit into an arbitrary 2D embedding. We perform Barnes-Hut tSNE on each of the suspects against the template networks with the same hyperparameters; namely, PCA initialization, 500 iterations, perplexity $= 1/3 * \sqrt{\# \, observations}$, theta = .5.

3.4 Animating across time

To further examine the network in detail, animations across time were produced based on procurement transactions. The name of each node was changed to the letter for better readability, followed by extra letters to indicate whether its edge name was sell or purchase and whether it was the template or the suspect.

Figure 4 is the last frame of the animated bar chart aggregates weight across time in descending order within each time period. Dark green represents the cumulative weight of the last frame, while light green represents the incremental weight of the current time period.

The scatter plot, figure 5, is the last frame aggregating weights of the procurement channel, faceting on the remaining networks. The grey bar at the bottom shows the progression of time for the current frame.

[*] e-mail: nicholas.spyrison@monash.edu
[†] e-mail: mkim0021@student.monash.edu
[‡] e-mail: andrew.pham@monash.edu

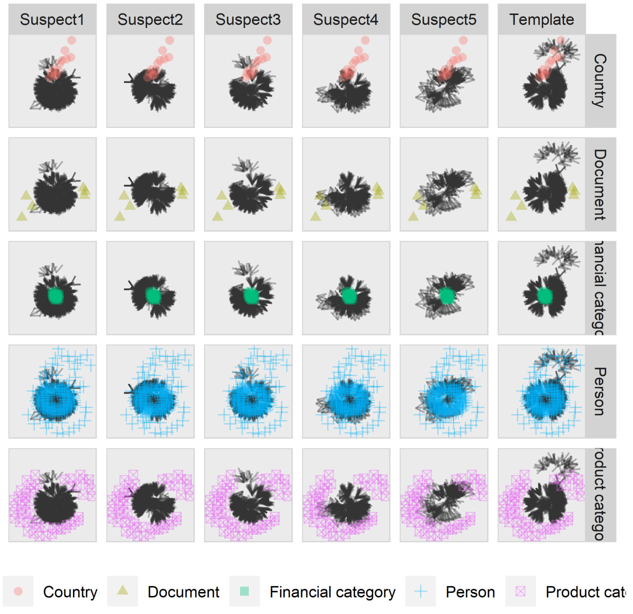

Figure 2: Network graph of each subset network across node name. This layout was generated from the 'largely' layout of the {igraph} R package. Click the image for a larger variant on our GitHub repository. The template network has the bulk of transactions happening in the densest region of the network pointing inward while having some outward-facing transactions going to nodes in low-density regions. Suspects 4 and 5 are comprised mostly of outwards facing transactions and they look quite different from the template network. Suspects 1, 2, and 3 have mostly inward trending transactions. They also exhibit a smaller fraction of outward transaction except for suspect 2.

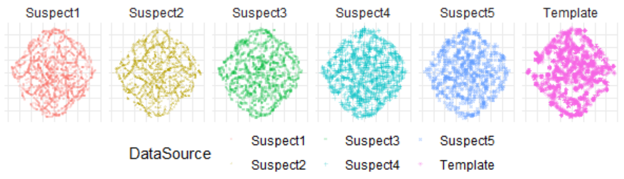

Figure 3: tSNE non-linear embedding of each subset network. Template network has medium length strings and clusters of points. No suspects have such clustering of points. Suspects 1, 2, and 3 have suitable stringiness, while suspects 4 and 5 strings are short and choppy. Click on the image for a larger web version.

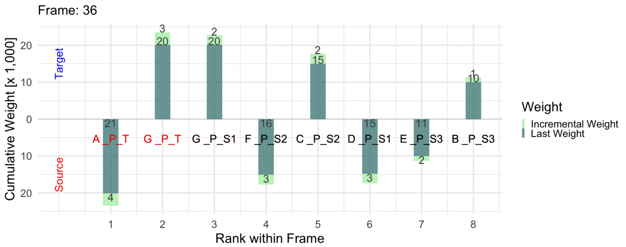

Figure 4: The final frame of the cumulative and incremental summation of procurement weights of the target, suspect 1, 2, and 3 networks. Each bar is a node within the top 10 sum of procurement weights within the given frame. Click on the figure to view the full .gif animation across time on the web.

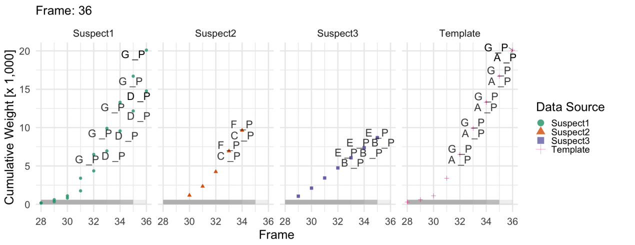

Figure 5: The final frame of the animation aggregating the weights of procurement transactions for the target, suspects 1, 2, and 3 networks. Each data point represents procurement weights at a particular frame. Click on the figure to view the full .gif animation across time.

4 Conclusion

In mini-challenge 1 we are asked to compare and contrast the 5 suspect networks with a target, template network. This template network has been verified by domain experts to contain true malicious behavior of the type we are trying to identify in such a cyberattack. Following our application of Shneiderman's mantra, we draw the following conclusions:

First, we take a higher-level overview in figure 1, we find the distributions of the data sources are similar enough for like-comparison. Zooming-in we visualize the networks across dataset and channel in figure 2 and in a non-linear, 2D projection space in figure 3. Both approaches corroborate that suspects 4 and 5 do not behave like the template network; we remove these candidates from our search. Figure 2 further shows that suspect 2 does not have a small volume of transactions coming outward from the dense center that is found in suspects 1, 3, and the template network. While figure 3 shows that clustered behavior of the template network is absent from the embedding of suspects 1, 2, and 3. To allow for details on demand we produced bar charts and scatter plots animated across time to take a closer look at the temporal behavior of individual channels or networks.

We feel confident that suspects 4 and 5 do not exhibit malicious behavior as identified by the template. Suspect 2 is less suspicious as is missing a notable feature present in the template that is present in suspects 1 and 3. We also note a feature that is unique to the template, but not present in any suspect. We recommend conferring with domain experts on a couple of points. First, we want to validate if the outward trend absent from suspect 2 is a necessary feature of such malicious behavior. If so, this would preclude suspect 2 from the search. Secondly, we want to identify if the clustering behavior identified uniquely in the template network is necessary for target behavior. If so, this lends evidence that even suspects 1 and 3 lack a necessary feature of the malicious behavior in question; if this is the case, we may need to broaden the search outside of the 5 suspects to find the true culprits responsible for the attack.

5 Software

The work for this paper was performed in R [4], using the packages {dplyr} [8], {gganimate} [3], {ggplot2} [7], {ggraph} [2], {Rtsne} [1], {tidyr} [9]. For larger variants of any of the figures, click on that figure to bring up a larger version hosted on GitHub. All code, figures and their variants can be found on our GitHub repository github.com/nspyrison/VAST_Challenge_2020/.

References

[1] J. H. Krijthe. *Rtsne: T-Distributed Stochastic Neighbor Embedding using Barnes-Hut Implementation*.

[2] T. L. Pedersen. *ggraph: An Implementation of Grammar of Graphics for Graphs and Networks*.

[3] T. L. Pedersen and D. Robinson. *gganimate: A Grammar of Animated Graphics*.

[4] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing.

[5] B. Shneiderman. The eyes have it: A task by data type taxonomy for information visualizations. In *Proceedings 1996 IEEE symposium on visual languages*, pp. 336–343. IEEE.

[6] L. van der Maaten and G. Hinton. Visualizing data using t-SNE. 9:2579–2605.

[7] H. Wickham. *ggplot2: Elegant Graphics for Data Analysis*. Springer-Verlag New York.

[8] H. Wickham, R. François, L. Henry, and K. Müller. *dplyr: A Grammar of Data Manipulation*.

[9] H. Wickham and L. Henry. *tidyr: Tidy Messy Data*.