https://doi.org/10.48009/2_iis_2019_195-205

Issues in Information Systems
Volume 20, Issue 2, pp. 195-205, 2019

MAPPING THE STRUCTURE OF A TWITTER "SECURITY EXPERT" SOCIAL NETWORK

John E. Anderson, Utah Valley University, janderson@uvu.edu
Daniel McDonald, Utah Valley University, Daniel.McDonald@uvu.edu

ABSTRACT

The researchers used a writer's list of favorite "security experts to follow" to seed a Twitter network and analyze whether the recommended experts were indeed amongst the most influential "security experts" on Twitter. They analyzed the resulting Twitter network to find the most important nodes in terms of popularity, quality of connections, types of roles played, such as bridges between groups, and node ability to quickly spread information. They found that only some of the recommended security experts appeared most influential given the network analysis. They also found that the experts on the list were often the centers of sub-groups. They concluded that starting with a writer's favorite list of experts may be helpful in seeding a more comprehensive list.

Keywords: Twitter Security Expert Network, Social Network Analysis

INTRODUCTION AND LITERATURE REVIEW

Making lists of people to follow on Twitter (opinion leaders or influencers) to keep up-to-date on the latest news in a professional community has become quite popular. Vonnegut (2014, 2015), Vartabedian (2015), and Baig (2017) have created several personal favorite lists of information security influencers to follow on Twitter. Personal favorite lists are influenced by frequency of tweets, jobs and experience of experts, reputations of the experts outside of Twitter, along with the individual preferences and biases of the list's creator.

Twitter is a social network created in 2006 that allows personal expression using small messages (microblogs) of between 140-280 characters. People can "follow" users without mandatory reciprocity resulting in communities (Grandjean, 2016). Currently Twitter has more than 300 million users (Twitter, 2018). Social networking sites facilitate information dissemination and aggregation, and leverage collaboration (Keckley & Hoffmann, 2010).

Studies on opinion leaders began many years ago (Katz & Lazarsfeld, 1955). Rogers (1962) defined opinion leaders as individuals who influence other people to adopt and disseminate an innovation. They are often journalists, public figures, or celebrities, who are considered highly informed, and well connected in the sphere in which they exert opinion leadership (Boster, Kotowski, Andrews, & Serota 2011) and thus have a disproportionate impact on the spread of information or behaviors (Bakshy, Hofman, Mason & Watts, 2011). Researchers have suggested that information diffusion may be maximized by seeding a piece of information with opinion leaders (Soumerai, McLaughlin, Gurwitz, Guadagnoli, Hauptman, Borbas, … Gobel, 1998).

A social network is a social structure made up of many types of interdependency between individual nodes (users, actors, vertices) making a larger web (Keenan & Shiri, 2009). Social network analysis (SNA) considers the social context of the node and the interaction (relations, tiles, edges) among the nodes (Knoke & Kuklinski, 1982). SNA is a popular approach to assess the patterns of relationships among users as well as the exchange of information among them showing how information moves and how users are positioned to control the information flow (Haythornthwaite, 1996). Common goals of SNA are finding important actors and discovering cohesive groups. Research questions are often: Who are the most central members of a network and who are the most peripheral? Which people have most influence over others? Does the community break down into smaller groups and if so what are they? Which connections are most crucial to the functioning of a group? (Newman, 2006).

RESEARCH QUESTIONS

Given a list of Vonnegut's (2015) personal favorite experts to follow, we developed two research questions. First, is whether the influence of the nodes from a list of personal favorites can be confirmed via a data-driven network analysis of those nodes on Twitter? Second, is whether the network analysis could generate additional useful recommendations of experts?

METHODOLOGY

Analyzing the structure of sub-networks in Twitter enables influencer identification and community discovery in a social network. We used the personal favorites list of Vonnegut (2015) which consisted of 16 CISOs and security leaders (see Table 1) to seed our Twitter analysis. We pulled the "following" and "follower graphs" of the 16 security leaders on the weekend April 13-15, 2018. This became the dataset for our analysis. We analyzed the downloaded graph using Gephi to calculate whole network measures, connection centrality measures, and path centrality measures. Using these metrics, we evaluated the personal favorite list for node influence as well as searched for additional node recommendations to create a more comprehensive list.

Table 1. Vonnegut's Personal Security Experts to Follow

Name and Twitter Handle	Background Information
Michael Coates (@_mwc)	Co-founder & CEO of @Altitude (Past CISO @ Twitter)
Alex Stamos (@alexstamos)	Teaching at Stanford (Past CISO of Facebook)
Martin Fisher (@armorguy)	IT Security at Northside Hospital CISO (southernfriedsecurity.com)
Zane Lackey (@zanelackey)	Formerly CISO @Etsy. Co-founder @SignalSciences. Author of Building a Modern Security Program
Andy Ellis (@csoandy)	@Akamai CSO
Myrna Soto (@myrna_soto)	COO, Venture Capital Partner at Trident Capital. Former CISO at Comcast Corp. & MGM Mirage
Jake Kouns (@jkouns)	CISO at @riskbased Founder @RVAsec (riskbasedsecurity.com)
Dave Kennedy (@hackingdave)	USMC. Founder, Senior Principal Security Consultant at @TrustedSec. Prior was CSO at Diebold Incorporated.
Nikk Gilbert (@nikkgilbert)	Tulsa, OK area. CISO, CSO at American Department of Defense, NATO, Alstom, ConocoPhillips, and the US Navy
Bruno Kerouanton (@kerouanton)	Switzerland, France, USA. co-founder and board member of non-profit Swiss Cybersecurity Label CyberSafe.ch. CISO of the Republic and Canton of Jura
Phil Cracknell (@pcracknell)	England, UK CISO. Runner-up - 2017 SC Awards - CISO of the year. Cyber-security personality of the year 2015/16 - http://cybersecurityawards.com/cyberwinners2015/
Dan Lohrmann (@govcso)	Holt, MI area. Chief Strategist and Chief Security Officer (CSO) for Security Mentor. Former Michigan CSO. 2017 Cybersecurity Breakthrough Award 'CISO of the Year' for security product and services companies.
Fortalice Solutions (@fortalicellc)	Theresa Payton (@trackerpayton) is CEO @ Fortalice Solutions
Jared Carstensen (@jaredcarstensen)	South Africa. CISO at CRH (Dublin, Ireland). author of the book "Cloud Computing: Assessing the Risks." Formerly a Sr. Manager at Deloitte
Darren Argyle (@d_argyle)	Sydney, Australia. former Group Chief Information Security Officer (CISO) at Qantas Airlines and, before coming to live in Australia, the former Chief Security Officer at IHS Markit, a global FinTech headquartered in the UK
Richard Rusing (@secrich)	Chicago, IL - CISO at Motorola Mobility

Network Analysis using Gephi

Gephi is open source software for network analysis, which allows for interactive exploration and visualization. (Bastian, 2009) Gephi implements several force-directed graph drawing algorithms which assign forces among a set of edges and nodes to attract pairs of endpoints to each other while also keeping each pair of nodes separate. Large complete networks are usually very complex and unreadable. Filtering is used to increase readability. These drawings often are beautiful, and produce crossing-free layouts in a planar graph. (Ji, 2015)

Whole Network Measures
Network diameter is the length of the shortest path between the most distanced nodes. It is used to measure the topology and concentration of a network, with a more concentrated network having a smaller diameter. (Ji, 2015)

Graph density is a measure of network cohesion (Webster and Morrison, 2004). It measures how close the network is to complete, or the actual number of links (edges) divided by the maximum number of links possible. A complete graph has all possible edges and a density equal to 1 (scale 0-1).

Modularity measures how well a network decomposes into modular communities. A high modularity score indicates a sophisticated internal structure of sub-networks. (Hammer, 2018) The modularity algorithm looks for nodes that are more densely connected together than to the rest of the network. (Paranyushkin, 2016)

Node Measures
Each node has several attributes that describe its importance. The most common attributes describing the importance of a node are the individual centrality measures (e.g. degree, closeness, betweenness, eigenvector) which analyze the position of an actor in a network.

Centrality Connections Measures
Degree centrality is a measure of the number of connections (direct one hop) each node has to other nodes within the network. In a directed graph, degree is divided into "indegree" and "outdegree" which count the incoming and outgoing edges, which are summed to make "degree." (Totet, 2013) Indegree is often interpreted as a kind of popularity, and outdegree as friendliness. In social settings, people with more connections may have more power.

Eigenvenctor centrality modifies degree centrality by weighting "quality" connections. It is a measure of a node's connection to well-connected nodes, or the "influence" of the node. It assigns nodes relative scores based on the normalized weighted sum of centralities of its neighbors, so that connections to high-scoring nodes contribute more to the score of that node than equal connections to low-scoring nodes, with a high score going to nodes that are connected to many other well-connected nodes. (Newman, 2006)

Centrality Network Path Measures
Betweenness centrality detects bridge nodes by counting the number of times a node acts as a bridge along the shortest path between two other nodes. (Freeman, 1977) It measures all the shortest paths between every pair of nodes on the network and then counts how many times a node is on a shortest path between two others. Nodes with a high betweenness centrality suggest that they are people that occupy an intermediate position between other people or groups, they connect various parts of the network together. It identifies nodes in the network that are crucial for information flow as a bridge. (Hirst, 2010) In social settings, a node with high betweennes exerts influence by virtue of not being in the middle but by lying between other nodes.

Closeness centrality is a measure of the closeness of a node to all other nodes in the entire network. (Sabidussi, 1966) It is the **inverse** average distance to every other actor. A node with a high closeness centrality means there is a short average distance between that node and the rest of the network, whereas a small closeness centrality means that there is a long average distance to the rest of the network. (Wolfram, 2015) It identifies nodes in the network that are crucial for the quick spread of information.

Eccentricity centrality measures the distance between a node and the node that is farthest away from it. It is a measure of the centrality of a node in a network based on having a small maximum distance from a node to every other reachable node (i.e. the graph eccentricities). High eccentricity centrality is given to nodes that are at short maximum distances to every other reachable node. (Wolfram, 2015) These nodes are strategically located to minimize distance traveled of information.

RESULTS

Security Expert Twitter Network Map
Figure 1 shows the security expert twitter map divided into communities.

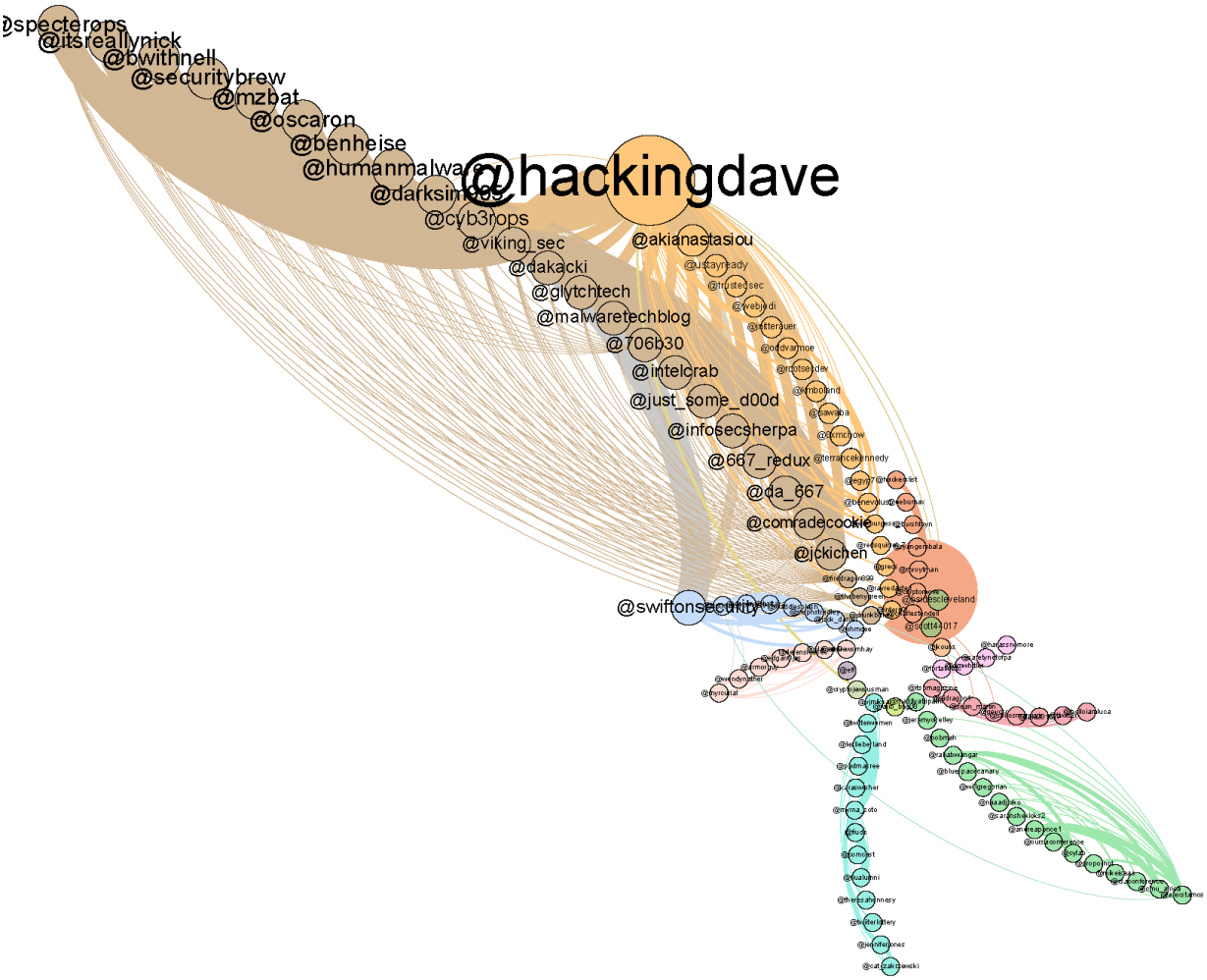

Figure 1: Security Expert Twitter Network

Whole Network Analysis
The graph had 363 nodes and 709 edges. For visualization purposes, to focus on the nodes of most importance we filtered out the nodes of degree 1 and 2 (about 68.9% of the nodes), leaving 113 nodes and 379 edges.

Table 2. Whole Network Measures

Network Measures	Entire Population	Filtered Population (degree 3-180)
Graph Density	.0005	.03
Average Degree	1.953	3.354
Network Diameter	7	6
Average Path Length	3.199	3.086
Modularity Classes	18	9

As seen in Table 2, the density of the network is low (.0005 for the full population and .03 for the filtered population) which show that it is **loose-knit** instead of densely connected. This suggests that actors within these networks are **following specific actors that they believe are important**. This is reinforced by the fact that the average degree of our entire network at 1.95 means that each node has only about 2 edges, which is quite low. Degree is the sum of the edges for a node or number of direct connections a node has.

The network diameter is the longest graph-distance between any two nodes in the network. The distance between the two most distant nodes in the network is 7 for the full population and 6 for the filtered population, with an average path length of about 3 for both.

Sub-graph Analysis
Modularity Classes is a community detection methodology that found 18 classes (communities) in the whole network and 9 in the filtered network. The connected components measure is also a way to detect the number of sub-graphs (or sub-communities) in a graph. For the entire population we detected possibly 11 sub-graphs and 8 sub-graphs for the filtered population. A sub-graph is a group who share a goal and have many stable contacts with each other.

User Analysis - The Security Experts
At the user level of analysis, we evaluate the location and grouping of actors in the network. We try to see who plays various roles in a network -- who are the connectors, mavens, leaders, bridges, isolates, where are the clusters and who is in them, who is in the core of the network, and who is on the periphery? (Orgnet.com/sna.html, 2019)
Of the original 16 security professionals in the list, 3 did not participate in twitter during the three days we pulled the data: Michael Coates (@_mwc), Jared Carstensen (@jaredcarstensen), Darren Argyle (@d_argyle). The 13 remaining are listed with their measures in Table 3 sorted by degree.

Table 3. Security Expert Node Measures

Label	friends_count	followers_count	indegree	outdegree	degree	eigencentrality	closnesscentrality	betweenesscentrality	Eccentricity	modularity_class
@hackingdave	4102	70356	26	36	62	1.00	0.55	1651.67	5	0
@csoandy	744	18487	9	11	20	0.51	0.40	1337.00	4	3
@alexstamos	1008	34147	12	4	16	0.12	0.29	642.00	5	9
@myrna_soto	406	2000	6	6	12	0.04	1.00	15.00	1	8
@armorguy	1053	9331	5	3	8	0.07	0.67	54.00	2	4
@govcso	NA	NA	7	0	7	0.02	0.00	0.00	0	6
@fortalicellc	7638	8662	3	0	3	0.01	0.00	0.00	0	10
@secrich	NA	NA	2	0	2	0.03	0.00	0.00	0	15
@nikkgilbert	12752	13276	0	1	1	0.00	1.00	0.00	1	17
@kerouanton	NA	NA	1	0	1	0.00	0.00	0.00	0	2
@pcracknell	NA	NA	1	0	1	0.00	0.00	0.00	0	16
@zanelackey	NA	NA	1	0	1	0.00	0.00	0.00	0	7
@jkouns	1140	3006	0	0	0	0.00	0.00	0.00	0	11

The first two columns are the counts of friends and followers. Friends_count is the “collection of user objects for every user the specified user is following (otherwise known as their "friends")” (Twitter, 2019). Follower_count is the “collection of user objects for users following the specified user” (Twitter, 2019). It is interesting that these counts, although related to degree, do not always predict degree.

Of the 13, we can see the five most important in terms of the number of connections (degree) each node has to other nodes within the network are @hackingdave, @csoandy, @alexstamos, @myrna_soto, and @armorguy sorted by degree largest to smallest. They are the most “popular” nodes. The same listing is maintained when we weight the “quality” connections (eigencentrality), except that @myrna_soto and @armorguy change places. They are the most “well-connected” nodes.

The same five act as bridge nodes, which we calculate by counting the number of times a node acts as a bridge along the shortest path between two other nodes. We can see that @hackingdave and @csoandy acted as a bridge over a thousand times, and @alexstamos over six hundred times. They are the nodes in the network that are most crucial for information flow because they lie between other groups of nodes.

The same five, along with the addition of @nikkgilbert, had a short average distance between themselves and the rest of the network (closeness centrality), in the same order excepting that @armorguy is the last. These same six also had the shortest maximum distances to every other reachable node (eccentricity) in the same order other than @armorguy

goes into fourth position. These nodes are crucial for the quick spread of information because they are strategically located to minimize the distance traveled of information.

Interestingly, all 13 security experts are in different modularity classes (or groups) in our network.

User Analysis - The Security Experts within the Larger Network
Next, we look at the security experts within the larger Twitter network.

Central Figures
Table 4 shows the top 25 nodes sorted by degree (on the left) and by eigencentrality (on the right). We see that only four our security experts made it on the degree list: @hackingdave, @csoandy, @alexstamos, @myrna_soto. We also note that their list positions are 1, 7, 9, and 12. There are other users of higher degree (more connections or more popular) in the list. We see that only two of our security experts made it on the eigencentrality list: @hackingdave, @csoandy. We also note that their list positions are 1, and 25. There are other users of higher eigencentrality (having higher quality connections) in the list.

Table 4. Whole Network Top 25 Nodes by Degree and by Eigencentrality

Label	indegree	outdegree	degree	Label	eigencentrality
@hackingdave	26	36	62	@hackingdave	1.00
@viking_sec	8	33	41	@benheise	0.858977
@darksim905	9	23	32	@bwithnell	0.858977
@jckichen	5	23	28	@humanmalware	0.858977
@comradecookie	5	23	28	@itsreallynick	0.858977
@firedragon899	0	24	24	@mzbat	0.858977
@csoandy	9	11	20	@oscaron	0.858977
@706b30	6	11	17	@securitybrew	0.858977
@alexstamos	12	4	16	@specterops	0.858977
@cryptomove	12	3	15	@swiftonsecurity	0.750191
@swiftonsecurity	10	2	12	@cyb3rops	0.744994
@myrna_soto	6	6	12	@darksim905	0.728144
@drunkbinary	0	12	12	@viking_sec	0.631011
@thebenygreen	0	11	11	@706b30	0.629101
@myrcurial	5	5	10	@667_redux	0.629101
@benheise	10	0	10	@da_667	0.629101
@bwithnell	10	0	10	@dakacki	0.629101
@humanmalware	10	0	10	@glytchtech	0.629101
@itsreallynick	10	0	10	@infosecsherpa	0.629101
@mzbat	10	0	10	@intelcrab	0.629101
@oscaron	10	0	10	@just_some_d00d	0.629101
@securitybrew	10	0	10	@malwaretechblog	0.629101
@specterops	10	0	10	@jckichen	0.533301
@sean_martin	3	6	9	@comradecookie	0.533301
@cyb3rops	9	0	9	@csoandy	0.51

Bridges
Table 5 shows that only 13 nodes acted as bridges (had betweennescentrality measures). Interestingly, 5 of our 13 security experts made it on the list: @hackingdave, @csoandy, @alexstamos, @armorguy, and @myrna_soto. They are the same as the top five sorted by degree listing above. We also note that there are others not in our seed list that act as bridges and are important because they are most crucial for information flow between groups of nodes.

Looking at the 35 nodes with closeness centrality (Table 5 in the middle), we see that only two our security experts made it on the list: @myrna_soto and @nikkgilbert. There are 33 other users with closeness centrality (having higher quality connections) in the list. Only two of our security experts are nodes in the network that are crucial for the quick spread of information based on their average distance to all other nodes.
However, looking at the 24 nodes with eccentricity values (Table 5 on the right), we see that five our security experts made it on the list: @hackingdave, @alexstamos, @csoandy, @armorguy, and @myrna_soto. We also note that there are other users with higher eccentricity scores (shortest max distance to every other node) in the list. These five of our security experts are nodes in the network that are strategically located for the quick spread of information, but there are others that also have good locations for the spread of information quickly.

Table 5. Whole Network Bridge Nodes (left) and Close Nodes by Closeness Centrality (middle) and by Eccentricity (right)

Label	betweenesscentrality
@hackingdave	1652
@csoandy	1337
@sawaba	703
@alexstamos	642
@swiftonsecurity	480
@myrcurial	232
@jnitterauer	124
@viking_sec	60
@armorguy	54
@darksim905	49
@myrna_soto	15
@twitterwomen	8
@sean_martin	1

Label	closnesscentrality
@scott44017	1
@cryptomove	1
@mroytman	1
@ryangembala	1
@myrna_soto	1
@fiudc	1
@itspmagazine	1
XXXXXXXXXXContinuedXXXXXXXX	
@dontaddressme	1
@pompili_f	1
@drerfanibrahim	1
@shadowcli	1
@nikkgilbert	1

Label	degree	eccentricity
@706b30	17	6
@drunkbinary	12	6
@thebenygreen	11	6
@jnitterauer	7	6
@hackingdave	62	5
@viking_sec	41	5
@darksim905	32	5
@jckichen	28	5
@comradecookie	28	5
@firedragon899	24	5
@alexstamos	16	5
@swiftonsecurity	12	5
@csoandy	20	4
@myrcurial	10	2
@armorguy	8	2
@twitterwomen	6	2
@cryptomove	15	1
@myrna_soto	12	1
@mroytman	9	1
@sean_martin	9	1
@ryangembala	8	1
@itspmagazine	8	1
@charlestendell	8	1
@fiudc	7	1

Table 6 shows each of the communities as assigned by modularity classes along with the node that is the center of community. Remarkably, we find that 10 out of our 13 security experts are the center of their groups. We also note that there are 8 other groups that have central nodes not on our security expert list, although 3 of our experts are in 3 of those groups.

Table 6. Network Communities

Modularity Class	Modularity Class Highest Degree
0	@hackingdave
1	@jnitterauer
2	@kerouanton*
3	@csoandy
4	@myrcurial
5	@maxsec
6	@cryptomove
7	@zanelackey*
8	@myrna_soto
9	@alexstamos
10	@fortalicellc
11	@govtechnews
12	@bsidescleveland
13	@akianastasiou
14	@network232
15	@secrich
16	@pcracknell*
17	@nikkgilbert*
*	with ties
	filtered network (degree 3 or more)
	security expert on list

DISCUSSION

One of the most interesting things we learned from the results of this study was that the personal favorites list of a security writer (Vonnegut 2015) which consisted of CISOs and security leaders she suggested security professionals should follow on Twitter, mapped to many of the most important nodes in the Twitter network we studied. There were five of the recommended group of 16 in particular that stood out as the most important: @hackingdave, @csoandy, @alexstamos, @armorguy, and @myrna_soto. These results support our first research question that a data-driven analysis of a Twitter network can confirm personal recommendations of users to follow.

While a personal list is not generated based on network analysis, not all the recommended Twitter users to follow were shown to be as important related to data-driven network measures as were the main five. Four different nodes were important in degree centrality, and two in eigencentrality. Information is spread in a network faster if a person with high degree hears the information and spreads it to many others (because they have so many friends). Also, a person of high degree is more likely to hear the information in the first place, because they have so many friends to hear it from. This is the concept of mean-square degree, a person with degree 10 is 10^2 or 10 x 10 = 100 times more efficacious at spreading the idea than a person with degree 1. The number of high degree nodes in a network also influences the spread of information. In fat-tailed degree distributions (with many nodes of high degree), the probability of each individual person spreading an idea can be small for the idea to spread through the whole community. Whereas in a slim-tailed degree distribution the probability of each individual person spreading the idea must be large for the idea to spread through the community. (Newman, 2006)

The main five users also acted as bridges. These five were also strategically located as far as having the shortest max path to all other nodes (eccentricity) to quickly spread information.

It is fascinating that all of the security experts on the list were part of different groups in the Twitter network, which might be a measure of the goodness or completeness or breadth of the list of Vonnegut. In the same vein, it was also surprising that 10 of the security experts where the centers of their Twitter groups (communities) in the network. This also supports the "goodness" of the Vonnegut's list.

Our second research question was whether the data-driven network analysis could create recommendations of users to follow that could contribute to a more comprehensive list. The data-driven analysis did indeed reveal many influential Twitter users to follow. By finding the central group nodes and bridge nodes in a larger Twitter network, we were able to identify who should be added to our list of "experts to follow". For example, new users that had strong rankings in both degree and eigencentrality (shown in Table 4) include the following: @viking_sec, @darksim905, @jckichen, @comradecookie, @706b30, @benheise, @bwithnell, @humanmalware, @itsreallynick, @mzbat, and @oscaron. Many of the above Twitter users also act as bridge nodes, namely @viking_sec, @darksim905, @jckichen, @comradecookie, and @706b30. There are also some new Twitter users that act as bridges including the following: @sawaba, @swiftonsecurity, @myrcurial, @sean_martin, and @twitterwomen. Adding all these users to a list of experts to follow makes sense because of the importance of their network positioning. Adding the recommended users helps ensure we follow a more complete breadth of security information professionals.

CONCLUSION

We were able to provide evidence for our first research question that a data-driven network analysis of Twitter users could validate a list of personal favorite recommendations. We started with a writer's list of suggested "security experts to follow". We then analyzed the network to find the most important nodes in terms of popularity, quality of connections, types of roles played, such as bridges between groups, and node ability to quickly spread information. We found that five of our security experts on the list were the most important on many measures. We also found that the experts on the list were often the centers of sub-groups. We were also able to provide evidence for our second research question as well that valuable recommendations of users to follow could be made from our analysis.

Several issues remain. Our analysis used time-bound data with a time constraint of data collected over a 3 day weekend Friday-Sunday period. It would be interesting to see if the network players stay about the same with data collected over a longer period. What is the content of the groups within the larger network? How is that content related to node importance? There are also questions of which measures are best to use in assessing node importance. For example, being that five of our security experts appeared on the eccentricity list and only two on the closeness centrality list, is eccentricity a better measure for a strategically located node than closeness centrality in expert information sharing?

REFERENCES

Baig, A., (2017). Top 5 Cybersecurity Influencers to Follow on Twitter in 2017. GlobalSign Blog. https://www.globalsign.com/en-sg/blog/top-5-cybersecurity-influencers-on-twitter/ posted July 28, 2017.

Bakshy, E., Hofman, J. M., Mason, W. A., & Watts, D. J. (2011 Feb 9-12) Everyone's n influencer: Quantifying influence on Twitter. WSDM'11, Hong Kong, China.

Bastian M., Heymann S., Jacomy M. (2009). *Gephi: an open source software for exploring and manipulating networks.* International AAAI Conference on Weblogs and Social Media.

Blondel, V. D., Guillaume, J., & Lefebvre, E. (n.d.). Fast unfolding of communities in large networks. (Modularity)

Boster, F. J., Kotowski, M. R., Andrews, K. R., & Serota, K. (2011). Identifying influence: Development and validation of the connectivity, persuasiveness, and maven scales. *Journal of Communication, 61,* 178-196.

Freeman, L.(1977). A set of measures of centrality based upon betweenness. *Sociometry. 40*(1), 35–41.

Grandjean, M. (2016). A social network analysis of Twitter: Mapping the digital humanities community. *Cogent Arts & Humanities, 3,* 1171458, http://dx.doi.org/10.1080/23311983.2016.1171458

Grandjean, M. (2015). *GEPHI – Introduction to Network Analysis and Visualization*, http://www.martingrandjean.ch/gephi-introduction/

Haythornthwaite, C. (1996). Social network analysis: An approach and technique for the study of information exchange. *Library & Information Science Research, 18,* 323-342.

Hammer, L., (2018) Modularity, https://github.com/gephi/gephi/wiki/Modularity accessed April 2019.

Heymann, S., (2015). Average Clustering Coefficient, https://github.com/gephi/gephi/wiki/Average-Clustering-Coefficient. Accessed April 2019.

Hirst, T., (2010) *Getting Started With Gephi Network Visualisation App – My Facebook Network*, Part III: Ego Filters and Simple Network Stats, https://blog.ouseful.info/2010/05/10/getting-started-with-gephi-network-visualisation-app-–-my-facebook-network-part-iii-ego-filters-and-simple-network-stats/

Ji, X., Machiraju, R., Ritter, A., & Yen, P. Y. (2015). Examining the Distribution, Modularity, and Community Structure in Article Networks for Systematic Reviews. *AMIA ... Annual Symposium proceedings. AMIA Symposium*, *2015*, 1927–1936.

Katz, E., & Lazarsfeld, P. (1955). *Personal Influence: That part played by people in the flow of mass communications.* New York, NY: The Free Press.

Keckley, P. H., and Hoffmann, M. (2010). *Social networks in health care: Communication, collaboration, and insights.* Deloitte issue brief. Retrieved July 2010 from http://www.deloitte.com/centerforhealthsolutions

Keenan, A., & Shiri, A. (2009). Sociability and social interaction on social networking websites. *Library Review, 58*, 438-450.

Kleinberg, J., (1998). Authoritative sources in a hyperlinked environment. Proc. 9th ACM-SIAM Symposium on Discrete Algorithms. Extended version in Journal of the ACM, 46(1999). http://www.cs.cornell.edu/home/kleinber/auth.pdf

Knoke, D., & Kuklinski, J. H. (1982). Network analysis. Sage University Paper Series on Quantitative Applications in the Social Sciences No. 07-028. Newbury Park, CA: Sage.

Newman, M. (2006). *The mathematics of networks* http://www-personal.umich.edu/~mejn/papers/palgrave.pdf Retrieved 2019-4-15.

Paranyushkin, D. (2016). *How can Modularity help in Network Analysis*, https://stackoverflow.com/questions/21814235/how-can-modularity-help-in-network-analysis accessed April, 2019.

Rogers, E. M. (1962). *Diffusion of innovations*. New York, NY: Free Press.

Sabidussi, G (1966). The centrality index of a graph. *Psychometrika, 31*(4), 581–603.

Social Network Analysis: An Introduction, http://orgnet.com/sna.html Accessed April 2019.

Soumerai, S. B., McLaughlin, T. J., Gurwitz, J. H., Guadagnoli, E., Hauptman, P. J., Borbas, C., … Gobel, F. (1998). Effect of local medical opinion leaders on quality of care of acute myocardial infarction. *Journal of the American Medical Association, 279*, 1358-1363.

Totet, M., (2013). *Let's Play Gephi: Understand Degree, Weighted Degree and Betweenness Centrality.* http://matthieu-totet.fr/Koumin/2013/12/16/understand-degree-weighted-degree-betweeness-centrality/

Twitter (2019). *Follow, search, and get users*, https://developer.twitter.com/en/docs/accounts-and-users/follow-search-get-users/api-reference/get-friends-list, accessed May 2019.

Vartabedian, J., (2015). *20 Top Security Influencers*. eSecurityPlanet https://www.esecurityplanet.com/network-security/20-top-security-influencers.html posted Jun 11, 2015.

Vonnegut, S., (2014). *21 AppSec & Security Gurus You Should Be Following on Twitter*. Checkmarx. https://www.checkmarx.com/2014/10/14/21-appsec-security-gurus-you-should-be-following-on-twitter/ Posted Oct 14, 2014.

Vonnegut, S., (2015). *16 CISOs and Security Leaders You should be Following on Twitter*. Checkmarx. https://www.checkmarx.com/2015/02/26/cisos-to-follow-on-twitter/ posted Feb 26, 2015.

Webster, C. M., & Morrison, P. D. (2004). Network analysis in marketing. *Australasian Marketing Journal (AMJ), 12*(2), 8-18.

Wolfram, (2015). *Social Network Analysis*, https://reference.wolfram.com/language/guide/SocialNetworks.html accessed April 2019.