Human Factors in Cybersecurity, Vol. 127, 2024, 52–62
https://doi.org/10.54941/ahfe1004765

A Notion of Trustworthiness Based on Centrality in a Social Network

Brian Dowtin[1], Kofi Kyei1[1], Yasmin Eady[1], A. M. Jackson[2], Bernard Aldrich[1], Joseph Shelton[2], and Albert Esterline[1]

[1]Computer Science Dept., North Carolina A&T State University, Greensboro, NC 27411, USA
[2]Computer Science Dept., Virginia State University, Petersburg, VA 23806, USA

ABSTRACT

We develop a measure of trustworthiness for members of a social network that supports collaborative effort in a domain. Edges represent explicitly declared friendships. The measure for a person is the geometric mean of their betweenness and eigenvector centralities in their network. The focus is on ranking people according to these values, which are normalized. We show the rankings of the people in an Erdős-Renyi (ER) network according to our measures. In experiments on Barabasi-Albert (BA) and Watts-Strogatz (WS) as well as ER networks, the average differences between the maximum and the minimum trustworthiness of the people are plotted against the independent variable of each model that results in an increasing number of edges. For the ER and WS networks, this difference decreased significantly and nearly linearly vs. the independent variable, but the trustworthiness values increase: it is harder to distinguish the trustworthy from the not trustworthy when all are pretty trustworthy. For the BA networks in contrast, this spread decreased to a minimum then increased. It is conjectured that, with an increasing number of edges, how embedded hubs are in the network becomes a dominant factor while non-hubs remain not very embedded. This measure has been used in defining a protocol for a group using a distributed authentication protocol to decide whether to admit a candidate, an example of how our work provides a secure way for people to collaborate that exploits human characteristics.

Keywords: Trustworthiness, Social networks, Network analysis, Security

INTRODUCTION

This paper develops a measure of trustworthiness for a social network. In our networks, nodes represent people, and edges represent friendships explicitly declared between two equal partners. Such a network is a structure that supports collaborative effort in a particular domain where the members share competences expected in that domain. Such a restriction is required for trustworthiness to be understood. De Meo *et al.* (De Meo, 2017) found that the trust networks they investigated had large numbers of reciprocated trust links, suggesting an underlying symmetric friendship relation. What is addressed is, not trust, but trustworthiness, the quality of being worthy of trust whether one's colleagues actually have a trust attitude toward one. In the literature, there are generally two approaches to assigning levels of trustworthiness in a social network: in terms of centrality, where the most trusted occupy the most central positions in the network, and in terms of local considerations (such as helpfulness of ratings). Research suggests that the former is predictive of the later (De Meo, 2017), and the notion developed here is based on centrality.

Our trustworthiness measure for a person is the geometric mean of their betweenness and eigenvector centralities in their network. In fact, raw values are not of primary interest. Rather, it is how the people in the network are ranked according to these values since the main application of this research is in selecting those who are most or least trustworthy. To that end, we work with normalized values of the centrality measures and their geometric mean so that the sum of the values for the people in a network is 1.0. Of interest as well is the difference between the maximum and the minimum trustworthiness of the people in a social network as (*caeteris paribus*) the greater this spread, the clearer the choice between trustworthy and not trustworthy.

We have used the concepts presented here with the WebID protocol to implement a protocol for vetting a candidate for a WebID group (Kyei, 2023). The weight an agent has in deciding whether to accept a candidate depends on their trustworthiness. The WebID protocol (Sambra, 2014) is a secure authentication protocol where a WebID is an HTTP URI that dereferences to a user's profile, which contains (among other things) structured data in RDF using the FOAF (Friend Of A Friend, prefix **foaf**) ontology; a **foaf:knows** triple links the subject to a friend, and we assume such relations are symmetric. Combining the **foaf:knows** triples from the profiles of all members in a group results in a social network supported by the protocol. Other sorts of secure social networks can be formed in various ways, and security can be enhanced by exploiting the trustworthiness of the members.

The remainder of this paper is organized as follows. The next section reviews related work, some on trust in general, more on centrality as a measure of trustworthiness. Following this, we develop the notion of the geometric mean of betweenness and eigenvector centrality as a measure of trustworthiness but also note issues with using betweenness centrality. The fourth section interprets the results of several experiments run using three standard models of randomly generated networks. We show the rankings of the nodes in one network determined by our measure and plot, for each model, the average size of the spread between the highest and lowest trust values as a function of the variable controlling the number of edges. The final section concludes and suggests future work.

RELATED WORK

In computer science, trust has several definitions depending on the context. Lewis *et al*. (Lewis, 1985) provide a psychological model and outline the process of trust violation and repair. Grandison and Sloman (Grandison, 2003) define trust as the quantified belief by the trustor in the competence, honesty, security, and dependability of a trustee in a specific context. Trust could also be defined as the connection between two parties, where one (trustor) will rely on the (expected) actions by the other (trustee) (Airehrour, 2016). According to Golbeck (Golbeck, 2005), "Trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to good outcome”. Trustworthiness is strongly connected to credibility of a network and control of network resources.

We represent symmetric declared friendship relations in a social network with an undirected graph composed of nodes that represent individuals and edges that represent these relations. We use the geometric mean of eigenvector centrality and betweenness as a measure of trustworthiness. These measures consider the node’s context within the entire network, unlike the in-degree centrality used in (Wang, 2013). Zahi and Hasson (Zahi, 2020) present a method for Trust Value Based on Interaction and Recommendations using Centrality Method (TVIRCM), which provides a measure for the trust value of a node in a social network using centrality measures and recommendation calculations. They use degree, closeness, betweenness and eigenvector centrality in calculating Direct Trust (DT) as a sum of weighted values and calculate indirect trust (IT) using the recommendation of neighbouring nodes; one’s overall trustworthiness is the sum of one’s DT and IT. Ramya and colleagues (Ramya, 2013) describe a method for finding a user’s “influentialty” in a network using betweenness centrality while removing distrust edges in the network. They then use a graph search algorithm to find the shortest trusted paths; users on such paths are deemed trustworthy. De Meo and colleges (De Meo, 2017) note that web platforms generally rate users using two measures, Helpfulness Based Reputation (HBR, based on how other users rate the helpfulness one’s reviews) and Centrality Based Reputation (CBR, based on the users connectedness or centrality in the network). CBR has a benefit of being easily calculable, while calculating HBR is more difficult. The authors show, using real-life datasets, that CBR scores accurately predict HBR. See the next section for more background.

TRUSTWORTHINESS VALUES BASED ON NETWORK CENTRALITY

We develop a notion of trustworthiness based on centrality measures since those influential in a social network and in a position to control network traffic are generally considered trustworthy. Our measure of trustworthiness meets these intuitions. In assigning levels of trustworthiness in a social network, De Meo *et al*. (De Meo, 2017) consider the usual centrality measures: degree centrality, closeness centrality, betweenness centrality, eigenvector centrality, and page-rank. They found eigenvector centrality the most helpful measure in predicting a local reputation/trust measure based on ratings. The closeness centrality of node n in graph G is the multiplicative inverse of the sum of the lengths of the shortest paths between n and all other nodes in G (Bavelas, 1948); we rule this out for our measure since it does not reflect the structure of the network. Page-rank is very similar to eigenvector centrality, so we skip it. Besides eigenvector centrality, we also consider betweenness centrality, which (see below) has intuitive appeal. A notion that is a restricted version of eigenvector centrality is that of Eigentrust (Kamvar, 2003), designed for peer-to-peer networks and assuming trust scores are transitive. Element t_{ij} of trust matrix $\mathbf{T}$ is defined in terms of the number of i’s downloads from j of authentic vs. fake files; i’s reputation is the i^{th} component of the leading eigenvector of **T**. This notion, however, is too restricted for us. Our concepts also apply to technological systems supporting the friendship relations assumed. In particularly, we have applied this analysis to communities of servers with RDF profile documents where edges are reciprocal **foaf:knows** triples.

In this section, betweenness centrality and eigenvector centrality are reviewed, and we argue that the two measures together meet the intuitive conditions. See (Newman, 2018) for a general presentation of centrality.) We then present the notion of the geometric mean of the two measures and argue that it is the appropriate way to combine the two measures for a measure of the centrality of a node in a social network meeting our expectations. Finally, we look at some possible problems with betweenness centrality as a measure of trustworthiness.

The betweenness centrality of a node n for a given graph or network G is defined as $\sum_{(s\neq n\neq t)} \frac{\sigma_{st}(n)}{\sigma_{st}}$ (Freeman, 1977). Here σ_{st} is the number of shortest paths between s and t and $\sigma_{st}(n)$ is the total number of shortest paths between s and t passing through n. The betweenness centrality of a node measures the extent to which it can regulate the interaction or flow of information among other nodes in the network. A node with high betweenness centrality acts as a gatekeeper among the nodes. High betweenness centrality indicates high importance. A highly important person can reach out most easily to others and is more effective in influencing network-based activity, and thus would be considered highly trustworthy.

To find the eigenvector centralities of the nodes in a network G with N nodes, we form the adjacency matrix of G, an N $\times$ N matrix $\mathbf{A} = (\mathrm{a}_{m,n})$ where $\mathrm{a}_{m,n} = 1$ if node m is connected to node n and 0 otherwise. Where **x** denotes the principal eigenvector of **A**, x_m denotes the eigenvector centrality of node m, the value indexed by m in **x**. This addresses the qualitative nature of the connections of the nodes in a network by finding how much influence each node has in the network based on the level of influence of the nodes to which it is connected. To have a high eigenvector centrality value, a node must have connections with other influential nodes in the network. Intuitively, eigenvector centrality is a measure of how influential a person is. It considers two features of a social network: "how many people you know" and "whom you know". It too, then, provides a reasonable measure of trustworthiness.

We combine our two centrality measures for node n to get a measure of the extent to which a node is determined to have a position in the social network that indicates that they are trustworthy. Our centrality measures gauge how important n is regarding regulation of efficient network traffic (betweenness centrality) and how influential n is (eigenvector centrality). To combine these measures, their geometric mean is used. Where x_n and B_n represent normalized eigenvector and betweenness centrality values of node n, respectively, we define their geometric mean as $G(n) = \sqrt{x_n B_n}$. This mean is concave and symmetric. The main reason we use this mean for combining centrality measures is the same reason the United Nations Development Programme switched to geometric mean for computing the Human Development Index (HDI) (United Nations, 2019). To wit, with the geometric mean, "a low achievement in one dimension is not linearly compensated for by a higher achievement in another dimension." It "reduces the level of substitutability between dimensions" while ensuring that a small decline in one measure has the same impact as a small decline in another. "Thus, as a basis for comparisons of achievements, this method is also more respectful of the intrinsic differences across the dimensions than a simple average".

Betweenness centrality, although it sounds convincing as a measure of trustworthiness, has some apparently counterintuitive features as such a measure. Most obviously, the betweenness centrality of a degree-one node is zero since there can be no flow through it. For example, for the path graph on four nodes with edges {0, 1}, {1, 2}, {2, 3}, {3, 4}, nodes 0 and 4 have betweenness centrality zero while the other nodes have positive betweenness centrality. In contrast, all these nodes have positive eigenvector centrality. Interpreting the betweenness centralities in terms of trust, there is no need to trust 0 and 4 to pass things along: any traffic involving 0 goes through 1, and any traffic involving 4 goes through 3. More disturbing, all nodes in a complete graph have betweenness centrality zero. Again, there is no need to trust anyone here to pass things along as every shortest path connecting a pair of nodes consists simply of the edge connecting those nodes: there is no flow through anyone.

EXPERIMENTS

We here present the results and interpretations of several experiments we have run using three standard models of randomly generated networks: Erdős-Renyi (ER), Barabasi-Albert (BA), and Watts-Strogatz (WS) networks. We are interested in the rankings of the nodes in a network determined by these measures. We show node rankings for an ER network according to betweenness centrality, eigenvector centrality, and the geometric mean of the two. We are also interested in the size of the spread between the highest trust value for a node in a network and the lowest trust value for a node in that network. We plot this spread for each of the three random models as a function of a variable that controls the number of edges in a network, holding the number of nodes fixed. We present below the results and interpretations for the ER, BA, and WS model, in that order. For references on models of randomly generated networks in general, (Newman, 2018) is authoritative on technical points, and (Easley, 2010) is on real-world issues.

The earliest model for generating random networks is the ER model (Erdős, 1959). Given n nodes, each possible edge has a fixed probability p of being present, independently of the other edges. For each pair of values for the parameters n and p, there is a family of networks. The degree distribution of a network is the number of nodes of the various degrees, plotted as a graph number-of-nodes vs. degree. The degree distribution of ER networks is Poisson, so the number of nodes decays exponentially with increasing degree. They thus do not account for the formation of hubs (nodes of high degree), which are often observed in social networks. ER networks also tend not to generate triadic closures (where neighbours of a node are neighbours of each other), which are also common in social networks. The NetworkX function used for random ER networks in this experiment is **erdos_renyi_graph** (***n***, ***p***) with ***n*** fixed at 20 and ***p*** varied as mentioned below.

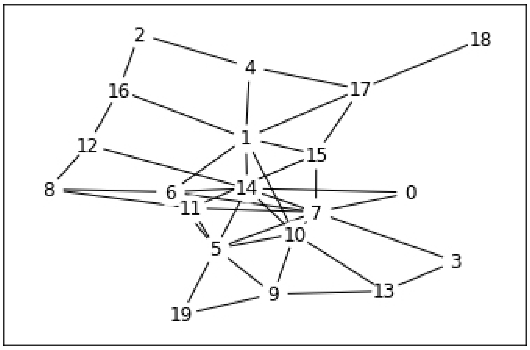

Figure 1: An ER network with n = 20, p = 0.2.

Table 1 lists the top six and bottom six nodes in the ER network with $p = 0.2$ shown in Figure 1 sorted in three ways, always by descending value: by betweenness centrality, eigenvector centrality, and the geometric mean of the two. Values are listed beside the nodes.

Table 1. Rankings of the nodes in Figure 1 by three measures.

Betweenness		Eigenvector		Geometric Mean	
Node	Value	Node	Value	Node	Value
1	0.218	7	0.106	1	0.140
7	0.112	5	0.099	7	0.119
10	0.108	14	0.099	14	0.110
14	0.103	6	0.092	10	0.105
5	0.087	10	0.085	5	0.102
17	0.080	1	0.075	6	0.078
			...		
8	0.009	19	0.027	13	0.019
3	0.007	3	0.025	3	0.015
2	0.003	16	0.021	2	0.006
0	0.000	4	0.021	0	0.000
18	0.000	2	0.008	18	0.000
19	0.000	18	0.005	19	0.000

Nodes 0, 18, and 19 have zero betweenness centrality and so also zero for the geometric mean. Node 18 is a degree-one node and ranks lowest in eigenvector centrality. Nodes 0 and 19 are degree-two nodes each at the vertex of a triangle whose opposite side provides a shortcut for flow to avoid the node, but these nodes do not have very low eigenvector centrality. (0, not shown, is ranked 10^{th} out of 20). Node 1 has high degree and the highest betweenness centrality, almost twice that of the next node. It, however, is toward the periphery of the graph. Its eigenvector centrality is not particularly high, but its betweenness centrality is so great that it ranks first in geometric mean. The node with the highest eigenvector centrality is 7. It has high degree and neighbours other nodes of high degree; it has the second highest betweenness centrality and geometric mean. The node with the second highest eigenvector centrality is 5, which also has high degree and neighbours high-degree nodes, but it ranks only fifth in betweenness centrality as the opposite sides in the triads it forms tend to shunt flow past it.

Figure 2 shows the average difference between the maximum and minimum value for nodes in ER networks with $n = 20$ and p from 0.2 to 0.7 by increments of 0.1. For each value of p, the difference between the maximum and the minimum value for a nodes was recorded for 100 generated networks, and the mean and standard deviation were computed. The plot shows the curve of mean values, and the error bars show the standard deviation above and below the mean. The geometric mean decreases significantly almost linearly. As the number of randomly placed edges in the network increases (with increasing p), few nodes with low centrality remain. The minimum value increases while the maximum changes little (as, even for small p, some nodes by chance are well embedded), and there is generally less spread in values (hence decreasing standard deviation). That the spread decreases is an indication that, with more randomly placed edges, truly untrustworthy nodes become rare.

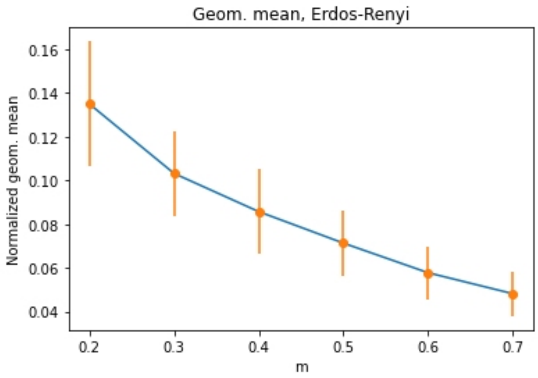

Figure 2: Average difference between max. and min. values of geom. mean vs. p for an ER network with n = 20 averaged on 100 runs for each p.

The Barabasi-Albert model for generating random networks (Albert, 2002) became popular for describing network formation based on popularity, such as is the case with the Internet, where hubs tend to form (Kleinberg, 2010). The degree distribution of a BA network is a power law, generally of the form $\frac{1}{k^c}$, where k is the degree and c is a constant (generally around 2 or 3). This decays much more slowly than the Poisson function for ER networks, thus accounting for hubs. Two major general concepts are captured by the Barabási–Albert model: growth (the number of nodes in the network increases over time) and preferential attachment (a new node attaches to an existing node with probability proportional to that nodes degree). The algorithm has one parameter, m, besides the final number of nodes. The network is initialized with at least m nodes, and at each step, a node is added and m existing nodes are selected as its neighbours with probability proportional to their degree. The BA model accounts for hubs but does not account for large numbers of triadic closures The NetworkX function used for random BA networks is **barabasi_albert_graph** (***n***, ***m***) with ***n*** fixed at 20.

Figure 3 is a plot generated like Figure 2 but for BA networks (instead of ER networks) where the independent variable is the parameter m. The code was executed for even integer values of m from 2 to 14. The curve is concave upward with maxima of c. 0.225 at $m = 2$ and $m = 14$ and a minimum of c. 0.150 at $m = 6$. The standard deviation steadily decreases with increasing m. The initial decrease in the spread might be expected as with the ER networks. Regarding the increase in the measure starting at $m = 6$, we conjecture that, with increasing m, how embedded hubs are in the network becomes a dominant factor while non-hubs remain not very embedded.

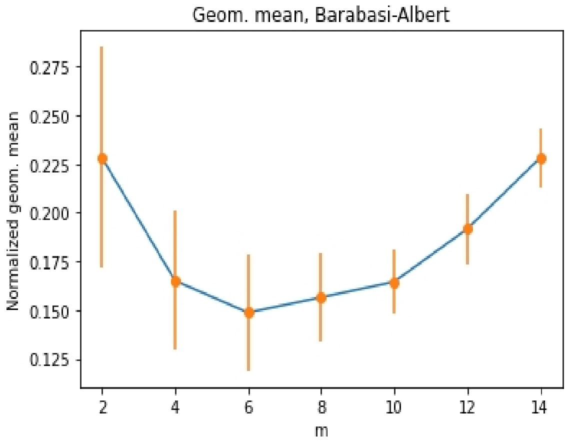

Figure 3: Average difference between max. and min. values of the geometric mean vs. m for a BA network with n = 20 averaged on 100 runs for each m.

Watts-Strogatz Networks

The *small-world phenomenon* is the idea that the world looks small when you consider how short the path of friends is from you to anyone. This idea was famously supported by a study by Milgram and colleagues (Travers, 1969) where each "starter" was given a letter to get to a "target" by forwarding through a chain of friends. Successful chains had a median length of six (the origin of "six degrees of separation"). The Watts–Strogatz model (Watts, 1998) is a random graph generation model that produces graphs with small-world properties and is the simplest model that overcomes the lack of triads found in ER yet retains the short average path lengths of the ER model. This model has two parameters (besides the number of nodes), K and p. The construction begins with a ring lattice (nodes can be arranged in a circle with each node connected to its nearest neighbours on the circle) each node of which has K neighbours, $K/2$ on each side. Then each lattice edge (u,

v) is "rewired" with probability p: replaced with a new edge (u, w) with uniformly random choice of existing node w. The lattice structure results in high clustering (a large number of triads) while the rewiring produces shortcuts. This model combines two fundamental social-network notions: homophily (that we are connected to others who are like ourselves) and the strength of weak ties (that mere acquaintances can provide information not available in our circle of friends—see (Granovetter, 1974)). Its major limitation is that it produces an unrealistic degree distribution, with a sharp peak at K. The NetworkX function used for random WS networks is **watts_strogatz_graph (*n*, *K*, p)** with ***n*** fixed at 20 and ***p*** at 0.2.

Figure 4 is a plot generated like Figure 3 but for WS networks (instead of BA networks) where the independent variable is the parameter K. Here, however, the values for the difference of the extremes for betweenness values alone (rather than for the geometric mean of the two centrality measures) are plotted since calculations for eigenvector centralities of WS generally did not converge. The code was executed for even integer values of K from 4 to 16. Like the curve for ER networks, this curve decreases roughly linearly, in this case, with K. While the independent variable in the ER plot is p and here it is K, we still note similarities. Apparently, the short path lengths of both the ER and the WS models are decisive here, and here again, as the number of edges in the network increases (with increasing K now), few nodes with low centrality remain. The minimum value increases while the maximum changes little, and there is generally less spread in values.

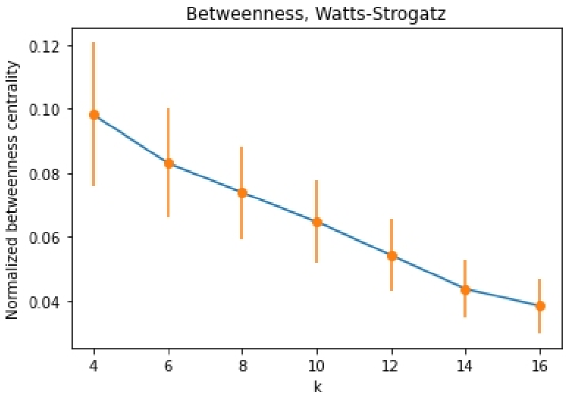

Figure 4: Average difference between max. and min. betweenness centralities vs. K for a WS network with n = 20, p = 0.2 averaged on 100 runs for each K.

CONCLUSION AND FUTUREWORK

This paper develops a measure of trustworthiness for members of a social network. Nodes represent people, and edges represent explicitly declared friendships. Such a network supports collaborative effort in a particular domain. This is trustworthiness (worthy of trust), not trust as an attitude to another, and our measure of it for a person is the geometric mean of their betweenness and eigenvector centralities in their network. We rank the people in the network according to these values and work with normalized values of the centrality measures and their geometric mean. We show the rankings of the people/nodes in an Erdős-Renyi (ER) network.

Our experiments use the Barabasi-Albert (BA) and Watts-Strogatz (WS) models for generating random networks in addition to the ER model. We note the average difference between the maximum and the minimum trustworthiness of the people in a social network since the greater this spread, the clearer the choice between trustworthy and not trustworthy. This difference is plotted against the independent variable of each model that results in an increasing number of edges for a fixed number (20 throughout) of nodes. For ER networks, this is the probability p of an edge between each pair of nodes, for BA networks, it is the number m of existing nodes selected (with probability proportional to their degree) as neighbors of each new node, and for WS networks, it is the number K of nearest neighbors to which each node in the initial ring lattice is connected. For the ER networks, the difference in trustworthiness scores decreased significantly and nearly linearly for p in the range [0.2, 0.7]. Note that the spread decreases but the trustworthiness values increase: it is harder to distinguish the trustworthy from the not trustworthy since everyone is pretty trustworthy. Similarly, the difference in scores for the WS networks decreased significantly and nearly linearly for K an integer from 4 to 16. For BA networks (which alone among the three models account for hubs), however, for m an integer from 2 to 14, the difference scores decreased significantly to a minimum at $m=6$ then increased significantly, at $m=14$ to about the value at $m=2$. We conjecture that, with increasing m, how embedded hubs are in the network becomes a dominant factor while non-hubs remain not very embedded.

We have used our measure of trustworthiness in defining a protocol for a group using the WebID distributed authentication protocol to decide whether to admit a candidate. Pairs of group members are linked by reciprocal **foaf:knows** triples in their RDF profiles representing declared friendships. These links are the edges in a technological network that supports a social network. In that application, the weight an individual has in the decision to admit a candidate into the group is determined by their trustworthiness measure. This is but one example of how the work reported here provides a secure way for people to communicate and collaborate. Humans are critical here as they form the social networks, which have a structure that supports measures of trustworthiness. In the future, we shall look for other applications of our measure in social networks, and we shall continue to investigate how our measure is sensitive to the formal characteristics of social networks, hoping to find additional general notions with real-world significance.

ACKNOWLEDGMENT

This research is based upon work supported by the ONR (Award No. N00014-22-1-2724). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

REFERENCES

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016) 'A lightweight trust design for IoT routing', *14th IEEE Intl Conf on Dependable, Autonomic and Secure Computing*, pp. 552–557.

Albert, R., & Barabási, A.-L. (2002) 'Statistical mechanics of complex networks', *Reviews of Modern Physics*, 74, pp. 47–97.

Bavelas, A. (1948). 'A mathematical model for group structures', *Applied Anthropology*, 7(3), pp. 16–30.

De Meo, P., Musial-Gabrys, K., Rosaci, D., Sarnè, G. M. L., & Aroyo, L. (2017) 'Using Centrality Measures to Predict Helpfulness-Based Reputation in Trust Networks', *ACM Transactions on Internet Technology*, 17(1), Article 8.

Easley, D., & Kleinberg, J. (2010) *Networks, crowds, and markets: reasoning about a highly connected world*. Cambridge University Press.

Erdős, P., & Rényi, A. (1959) 'On Random Graphs. I', *Publicationes Mathematicae*, 6(3–4), pp. 290–297.

Freeman, L. C. (1977) 'A set of measures of centrality based on betweenness'. *Sociometry*, 40, pp. 35–41.

Golbeck, J. (2005) *Computing and applying trust in web-based social networks*, Ph. D. Thesis, University of Maryland.

Granovetter, M. S. (1973) 'The Strength of Weak Ties'. *American Journal of Sociology*, 78(6), pp. 1360–1380.

Grandison, T., & Sloman, M. (2003) 'Trust Management Tools for Internet Applications', *International Conference on Trust Management*, pp. 91–107.

Kamvar, S. D., Schlosser, M., & Garcia-Molina, H. (2003) 'The EigenTrust algorithm for reputation management in P2P networks'. *International conference on World Wide Web* (*WWW'03*), ACM, pp. 640–651.

Kyei, K., Eady, Y., Esterline, A., & Shelton, J. (2023) 'Trust-based enrollment in a group in a distributed setting', *2023 ACM Southeast Conf.,* April 2023, pp. 120–127.

Lewis, J. D., & Weigert, A. (1985). 'Trust as a Social Reality'. *Social Forces* 63(4), pp. 967–985.

Newman, M. (2018) *Networks*. Oxford University Press.

Ramya, R., Parvathy, M., Sundarakantham, K., & Mercy Shalini, S. (2013) 'Trust Dependence Network for Recommender System', *International Conference on Advanced Computing* (*ICoAC*).

Sambra, A., Story, H., & Berners-Lee, T. (2014) *WebID, Web identity and discovery*. W3C Editor's Draft.

Travers, J., & Milgram, S. (1969). 'An experimental study of the small world problem'. *Sociometry*, 32(4), pp. 425–443.

United Nations Development Programme. (2019). *Frequently asked questions - human development reports*. Technical Report.

Wang, P. J., Bin, S., Yu, Y., & Niu, X. X. (2013). 'Distributed trust management mechanism for the internet of things', *2nd International Conference on Computer Science and Electronics Engineering* (*ICCSEE 2013*).