Trust levels in social networks

Santanu Acharjee\textsuperscript{a,*}, Akhil Thomas Panicker\textsuperscript{b}

\textsuperscript{a} Department of Mathematics, Gauhati University, Assam, India
\textsuperscript{b} Department of Physics, Cochin University of Science and Technology, Kerala, India

\section*{ARTICLE INFO}

\textbf{Keywords:}
Social networks
Uniform distribution
Power-law distribution
Power-law exponent
Trust
Dunbar's number
Evolutionary biology
Neocortex

\section*{ABSTRACT}

Dunbar’s number is the cognitive limit of an individual to maintain stable relationships with others in his network. It is based on the size of the neocortex of the human brain. On the other hand, trust is one of the major issues for one while selecting members for his social network and the evolution of his social network with time. Trust and Dunbar’s number are interconnected in the case of one’s stable social network. Trust needs time to be built after several social interactions, intimacy, etc. In this paper, we try to provide answers to the following important questions related to social networks:

(i) Do trust levels remain the same for individuals from one’s perspective in his social network when the network size increases?
(ii) What is the relation between the power-law exponent $\alpha$ and the trust cutoff?
(iii) Do trust levels help to diffuse information quickly or vice versa to reach Dunbar’s number 150 along with hierarchy layers of 5, 15, and 50 individuals in networks of different sizes?

We find that there is a requirement for trust levels to increase among the same individuals in one’s social network if the size of the network increases. As a relation between the power-law exponent $\alpha$ and the trust cutoff, it is found that $\alpha \propto 1/(\text{trust cutoff})$. Moreover, we also find that trust levels never help to diffuse information quickly or vice versa to reach Dunbar’s number 150, along with hierarchy layers of 5, 15, and 50 individuals in networks of different sizes.

\section*{1. Introduction}

“Social networks” is an area of interdisciplinary research that was developed from the ideas of graph theory \cite{1} in the last century. Erdős and Rényi \cite{2} laid the theoretical foundation of random graphs in 1960. Prior to 1999, it was believed that the social networks of individuals were nothing but random graphs \cite{3}. In 1999, Barabási and Albert \cite{3} disproved the existence of random graphs in several online networks, along with biological networks. After Barabási and Albert \cite{3}, the research area “Social networks” has grown to an interdisciplinary area. It is important to note that renowned graph theorist Frank Harary realized the importance of social networks several decades ago and thus made several contributions in Refs. \cite{4,5}. Moreover, it is easy to find connections between topology and social networks. One may refer to Refs. \cite{6–13} for recent research on topological aspects of social networks. Also \cite{14,15}, can be considered to find connections between social networks and computer science.

Trust helps to grow human social relationships \cite{16}. It binds individuals through benevolent acts and reciprocal interactions. Thus, it becomes the basis of friendship \cite{16,17}. According to Mitchell \cite{18}, trust is governed by social exchanges, viz., social presence, verbal and nonverbal communication, etc. In these types of social exchanges, the honesty or deception of the other party is assessed. A

* Corresponding author.
E-mail addresses: sacharjee326@gmail.com (S. Acharjee), atpanicker95@gmail.com (A.T. Panicker).

https://doi.org/10.1016/j.heliyon.2023.e19850
Received 17 April 2023; Received in revised form 29 August 2023; Accepted 4 September 2023
Available online 15 September 2023
2405-8440/© 2023 Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
psychological definition of trust can be found in Rotter [19]. In Ref. [19], Rotter defined trust as “an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied on”. Similarly, psychological definition of deception is stated as “a successful or unsuccessful deliberate attempt, without forewarning, to create in another a belief that the communicator considers to be untrue in order to increase the communicator’s payoff at the expense of the other side” [20].

Several theories on human friendship have suggested the importance of reciprocity and the exchange of benevolent acts in building social relationships [16,21,22]. Trust is one of the implicit factors in social relationships [16,21,22]. Experimental study by Hays [21] showed the advantages of investing resources on fewer but more intimate social relationships. Moreover, Granovetter [22] showed that weak ties often help to get more information and resources. According to Baumeister and Leary [23], mutual trust starts to grow between individuals, which leads to reliance on each other for emotional support, companionship, help, etc., when collaborations start to grow between the groups. Trust evolves to enhance collaboration in assessing the quality of trustworthiness or deception [24]. Hays [25,26] observed that close friendships have more weekly interactions, across a wider range of days, locations, and times than casual friendships. Close friends offer more informal and moral support than casual friends. Moreover, different dimensions for trust-oriented behaviors in friendships were classified, viz., positivity, openness, interaction and supportiveness. According to Sutcliffe et al. [27], best-friendships are found to be self-maintained. Roberts and Renwick [28] showed that the reputations of individuals based on their histories of collaboration help to build their social relationships.

Nowak and Sigmund [29] established that, in the case of a computer simulated repeated prisoner’s dilemma, cooperative strategies spread in populations if histories of interactions are assessable. In the case of socio-cognitive models of trust, several factors influence trusting relationships [30,31]. Falcone and Castelfranchi [30,31] identified the degree of delegation between two parties, risks, the motivations and goals shared by parties for social relationships, and reputations as the factors that influence trusting relationships. One may refer to Castelfranchi and Falcone [32] for more elaboration on social trust. Moreover, it is found that indirect reciprocity encourages social relationships and helps to form groups [33].

There are several studies on trust from the computational aspects. Sutcliffe and Wang [34] described the process of the development of social relationships using a computational model. Sutcliffe et al. [17] presented a social trust model to investigate the relationship between social networks and social relationships in real life and in social media. They found the existence of a few strong relationships in multilevel social structures. Their results demonstrated the existence of more medium ties and a large number of weak ties if one rewards well-being and alliances with high-level social interactions. Interested readers may refer to Ref. [17] for extensive literature on trust and related computational models. For recent research on trust in the cases of Facebook and Twitter, one may refer to Sabatini and Sarracino [35] and many others.

Both trust and deception are topics of equal interest to social scientists, economists, and network scientists. Gneezy [36] discussed the role of consequences through deception in economics. According to Gneezy [36], most economic interactions include deceptions. The extreme condition of economic theory assumes each agent is “homo economicus” during economic interactions. It means that each agent acts selfishly during economic interactions and does not bother about the well-being of others. Thus, deception is one of the major properties of selfish acts by an economic agent. For example, Akerlof [37] found that car sellers always lie for their own benefit in cases of asymmetric information. A similar argument in mechanism design [38] says that people trust if there are scopes for material outcomes as incentives. From the perspective of utilitarian philosophy, Bentham [39] argued that an individual must weigh benefits against harm, happiness against unhappiness, etc. before telling a lie. But a contradictory view of utilitarian philosophy came from Bok [40]. According to Bok [40], there is no difference between a truthful statement and a lie if both achieve the same monetary payoff. Thus, from Refs. [39,40], we can claim that we must be cautious when trusting individuals in our social networks?

There are four types of lying [36,41]. They are (i) pro-social; (ii) self-enhancement; (iii) selfish; and (iv) antisocial. Gneezy [36] suggested that people consider gain at the time of telling lies. Moreover, people also care about the loses of others along with their own gains. Serota et al. [42] conducted an experiment with 1000 Americans, and it was found that on average 1.65 lies were told by each American per day. Similarly, other experiments [43–46] proved that lies were told between frequency 0.6–2.0 per day, where face-to-face intersections had a lower chance of deception in comparison to telephonic conversations. Gino and Pierce [47] conducted experiments and found that people opt for dishonest behavior to relieve emotional distress caused by wealth-based inequity. Moreover, people increase hurting behavior and reduce helping behavior in the case of their own experiences of negative inequity or negative emotions, and they also increase dishonest helping behavior when they experience positive inequity or positive emotions [47]. Arnamolbi et al. [48] modelled the trusted information diffusion pattern in online social networks with the assumption that two nodes had trusted ties with reciprocal behavior. They showed that up to only 3% of ties are used in the case of information diffusion if there are strong ties in online social networks. They also found that in the case of trustworthy paths for communications in online social networks, two individuals are more than twice as far away from each other. Wang et al. [49] experimentally proved that badness influences psychological reactions more than goodness, but goodness influences behavior more than badness. Similar results were predicted by Panasiti et al. [50]. In the case of deception, one’s own reputation encourages other individuals in his social networks to be honest [50]. Moreover, they found that unfavorable situations motivate one to deceive in a stronger way. Gino et al. [51] conducted three experiments and concluded that individuals cheat more when their lies benefit others and when the number of beneficiaries from their lies increases. There are several studies on trust and deception. Trust and deception have a very strong connection with individual’s social networks in terms of Dunbar’s number.

There are mainly two approaches to studying social networks. One is “six degrees of separation” or “small world phenomenon” [52,53] and the other is Dunbar’s number [54]. Small world phenomenon focuses on the maximum number of intermediate acquaintance links needed to connect any two individuals. On the other hand, Dunbar’s number [54,55] is based on human cognition’s limit to maintaining stable relationships with individuals in one’s social network. Dunbar’s number is one of the fundamental factors of ego-centric social networks. Based on correlative studies of the size of social networks and neocortex sizes in the brains of primates and
humans, Dunbar [54] found that an individual can maintain stable relationships with only 150 individuals in his social networks. This was previously found for offline social networks, but the existence of the same result was confirmed, after the evolution of the internet, in the case of online social networks [25,56]. Dunbar’s hierarchy layers consist of alters with scaling ratio of 3 [57,58]. These hierarchy layers consist of a series of concentric circles of acquaintanceship [56,59]. An individual is placed at the centre of these hierarchy layers, and the remaining concentric circles consist of 5, 15, 50, 150, 500, 1500, and 5000 individuals cumulatively [56,59]. The hierarchy layers consist of 5 and 15 individuals are called support cliques and sympathy groups, respectively. Stiller and Dunbar [59] found that individual differences in social cognition explain the size of an individual’s support clique in a better way. On the other hand, the size of the sympathy group is well explained by an individual’s performance on memory tasks. Moreover, Dunbar [60] showed that six degrees of separation does not necessarily mean that information flows at a uniform rate in one’s social network. For recent review on Dunbar’s number, one may refer to Ref. [61]. From Refs. [49,60], we can ask the following questions:

(i) Do trust levels remain the same for individuals from one’s perspective in his social network when the network size increases?
(ii) What is the relation between the power-law exponent \( \alpha \) and the trust cutoff?
(iii) Do trust levels help to diffuse information quickly or vice versa to reach Dunbar’s number 150 along with hierarchy layers of 5, 15, and 50 individuals in networks of different sizes?

2. Uniform distribution of trust

In this section, we try to find the nature of one’s trust levels with acquaintances in his social network when the size of the network starts to increase. Let us consider a social network with a population of \( N > 1 \) individuals and each of them has an initial trust value \( x \), where \( x \in [0,1] \). We consider a constant \( T_c \in [0,1] \) as the critical value of trust for an individual, above which he is susceptible to receiving information as well as transmitting information to others. The individuals below the critical value of trust \( T_c \) are considered non-reliable by their neighbors, and thus they don’t participate in information transmission. Based on individuals’ roles in information transmission, we divide the population into three categories. They are given below.

1. Susceptible (S),
2. Ignorant (I),
3. Transmitters (R).

The susceptible (S) people are those individuals who can receive information and become a transmitter (R). The ignorant (I) category consists of individuals with trust value below the critical value of trust \( T_c \). We assume \( \beta \) as the rate of diffusion with which a transmitter sends information to neighboring susceptible individuals. In this paper, we are considering two types of distribution for trust on individuals. One is uniform distribution, and the other is power-law distribution.

Now, we consider that all individuals are assigned trust values, which are selected from a uniform distribution in \([0, 1]\). Let \( f \) be the fraction of people with a trust value greater than or equal to \( T_c \). Hence, the effective number of susceptible individuals is \( S = Nf \). In the case of uniform distribution, the fraction of the population that participates in information diffusion is \( f = 1-T_c \) and the fraction of the non-reliable or ignorant population is \( 1-f = T_c \). Thus, dynamic equations regarding the information diffusion in our case are given below.

\[
\frac{dt}{dt} = 0
\]

\[
\frac{dS}{dt} = -\beta SR/N
\]

\[
\frac{dR}{dt} = \beta SR/N
\]

To normalize the dynamics equations, we consider \( \frac{N}{N} = s \). Hence, we obtain \( s = f \). Now, we consider \( \frac{N}{N} = r \). So, at any instant \( t \), we obtain \( \frac{1}{N} = 1-f \cdot r \). If we denote \( \frac{1}{N} = i \), then \( i + f \cdot r = 1 \). Thus, dynamic equations (1)–(3) are reduced to the following equations (4)–(6):

\[
\frac{di}{dt} = 0
\]

\[
\frac{df}{dt} = -\beta fr
\]

\[
\frac{dr}{dt} = \beta fr
\]

Since \( f = 1-i \cdot r \), thus equation (6) becomes

\[
\frac{dr}{r(1-i-r)} = \beta dt.
\]
We consider $r = r_0$ at $t = 0$. As $r$ is time dependent, hence the solution of (7) becomes

$$r(t) = \left( \frac{e^{(1-i)\beta t} (1-i)r_0}{1 - i - r_0 + r_0 e^{(1-i)\beta t}} \right).$$  

(8)

It is a logistic solution of equation (7) with an initial fraction of transmitters as $r_0$. If $t \to \infty$, then $r(t) \to 1 - i$. Thus, every susceptible individual gets the information and becomes a transmitter. When $i = 0$ at $t = 0$, then equation (8) reduces to the following:

$$r(t) = \left( \frac{e^{\beta t} r_0}{1 - r_0 + r_0 e^{\beta t}} \right).$$

(9)

Thus, from equation (9), we obtain the fraction of transmitters at any instance $t$ with an initial fraction of transmitters $r_0$ in our social network with $N$ (>1) individuals.

3. Power-law distribution of trust

According to Barabási and Albert [3], large networks, viz., the WWW, citation patterns in science, the collaboration graph of movie actors, etc., are scale-free networks. In a scale-free network, the probability $P(k)$ that a vertex in the network interacts with $k$ other vertices decays as the power-law is directly proportional to $k^{-\alpha}$, i.e., $P(k) \propto k^{-\alpha}$, with an additional requirement of $2 < \alpha < 3$.

Prior to Ref. [3], Redner [62] found the existence of power-law distribution in the citation distribution of published papers having the power-law exponent $\alpha \approx 3$. In order to generate a power-law distribution of trust with an exponent $\alpha$ from a uniform distribution $P_y$ in $[x_0, x_1]$, the random variable is given by,

$$X = \left[ \left( x_1^{\alpha-1} - x_0^{\alpha-1} \right)y + x_0^{\alpha-1} \right]^{(\alpha+1)^{-1}}.$$  

(10)

Equation (10) is the probability distribution function $P(x)$ for generating power-law with $x_0$ as the minimum value and $x_1$ as the minimum value and $x_1$ as the minimum value.

Fig. 1. (i) Diffusion of information among 150 people with different trust cutoff values and $\beta = 0.25$, (ii) diffusion of information among 150 people with different trust cutoff values and $\beta = 0.50$, (iii) total informed people with different trust cutoff values between 0 and 1, with an increment of 0.01 to visualize Dunbar’s hierarchy levels of stability and required trust values for 150 people, (iv) diffusion of information among 500 people with different trust cutoff values and $\beta = 0.25$, (v) diffusion of information among 500 people with different trust cutoff values and $\beta = 0.50$, (vi) total informed people with different trust cutoff values between 0 and 1, with an increment of 0.01 to visualize Dunbar’s hierarchy levels of stability and required trust values for 500 people.
maximum value of $x$. The minimum value of $x$ cannot be zero for a power-law distribution. So, we are fixing the minimum value of $x$ as 0.1 and the maximum value of $x$ as 1. Now, the minimum value of $x = 0.1$ means the minimum value of trust in the distribution cannot be lower than 0.1. For the critical value of trust $T_c$, in order to find $f$ in the case of power-law distribution, the fraction of individuals with trust values less than $T_c$ is obtained and is subtracted from 1. The probability distribution curve is obtained for $10^6$ values of $y \in [0.1, 1]$ to get a smooth curve for power-law distribution with the power-law exponent $\alpha$. Using the data from the probability distribution of the power-law and by fixing $T_c$, we can obtain the initial fraction $f$ of population who are susceptible with trust values greater or equal to $T_c$. The fraction $f$ can be used to find the number of susceptible people in the information transmission by $S = Nf$. Thus, fraction of people in the ignorant category is $i = 1 - s$. The remaining dynamics and equations are the same as for a uniform trust distribution.

4. Results and discussions

This section consists of discussions regarding Figs. 1–5. The following conclusions are drawn from simulations. They are providing answers to the questions of Section 1.

We first considered equation (9) to do simulations. For simulations, we used the programming language R version 4.3.0. Since, we are considering Dunbar’s hierarchy, thus initially at time $t = 0$, there is only one transmitter of an information. The one transmitter of information is due to the existence of ‘ego’ in Dunbar’s hierarchy [60].

![Fig. 2.](image-url)

(i) Diffusion of information among 1500 people with different trust cutoff values and $\beta = 0.25$, (ii) diffusion of information among 1500 people with different trust cutoff values and $\beta = 0.50$, (iii) total informed people with different trust cutoff values between 0 and 1, with an increment of 0.01 to visualize Dunbar’s hierarchy levels of stability and required trust values for 1500 people, (iv) diffusion of information among 5000 people with different trust cutoff values and $\beta = 0.25$, (v) diffusion of information among 5000 people with different trust cutoff values and $\beta = 0.50$, (vi) total informed people with different trust cutoff values between 0 and 1, with an increment of 0.01 to visualize Dunbar’s hierarchy levels of stability and required trust values for 5000 people.
Now, we discuss Fig. 1 (i-vi). For (i) to (iii) of Fig. 1, we are considering a network of 150 (\(\approx N\)) individuals with uniform trust distribution. Information is transmitted with transmission rates \(\beta = 0.25\) and \(\beta = 0.50\) in (i) and (ii), respectively, with \(R = 1\) at \(t = 0\), i.e., \(R_{t=0} = 1\). The total informed people level reaches Dunbar’s hierarchy levels of 50, 15, and 5 at trust values of 0.66, 0.90, and 0.96, respectively. In (ii), the diffusion occurs quicker with \(\beta = 0.50\) than with \(\beta = 0.25\) in (i). To get (iii) of Fig. 1 and similar figures, we used the simulation methodologies described in Section 2. In Fig. 1, (iii) represents the total number of informed people for all the trust cutoff values between 0 and 1, with an increment of 0.01 so as to easily visualize Dunbar’s hierarchy levels of stability and required trust values. In the cases of (iv) to (vi) of Fig. 1, we are considering a network of 500 (\(\approx N\)) individuals with uniform trust distribution. Information transmission rates are the same in (iv) and (v) as in (i) to (iii) in Fig. 1. Now, we can see from (vi) that at trust values 0.7 and 0.9, the total informed people level reaches Dunbar’s hierarchy levels of 150 and 50, respectively. Moreover, like a network of \(N = 150\) individuals, the diffusion of information occurs quicker at \(\beta = 0.50\) than at \(\beta = 0.25\) for a network of \(N = 500\) individuals.

In this paragraph, we analyze Fig. 2 (i-vi). We consider a network of 1500 (\(\approx N\)) individuals with a uniform trust distribution for (i) and (ii) of Fig. 2. We can see that at a trust value of 0.9, the total informed people level reaches Dunbar’s hierarchy level of 150. Like the previous two networks, it can be concluded from (i) and (ii) of Fig. 2 that information diffusion occurs quicker at \(\beta = 0.50\) than at \(\beta = 0.25\). As we extend our network size from 1500 to 5000 in (iii) to (vi) of Fig. 2, we find from (vi) that trust level increases to 0.97 to reach the stable connections of the network, i.e., Dunbar’s number 150. Moreover, information diffusion properties remain the same for \(\beta = 0.50\) as in our previous networks. From the above four network sizes, it is important to note that trust levels remain the same irrespective of the information diffusion rate in a network. It means that trust levels never help to diffuse information quickly or vice versa to reach Dunbar’s number 150, along with hierarchy layers of 5, 15, and 50 individuals in networks of different sizes.

Fig. 3. (i) To maintain trust among the same 5 people; trust levels require 0.97 and 0.99 once the network size increases to 150 and 500 people, (ii) to maintain trust among the same 15 people; trust levels require 0.90 and 0.97 once the network size increases to 150 and 500 people, (iii) to maintain trust among the same 50 people; trust levels require 0.66 and 0.90 once the network size increases to 150 and 500 people, (iv) to maintain trust among the same 150 people; the trust level increases from 0.70 for a network of 500 people to 0.90 for a network of 1500 people, (v) to maintain trust among the same 500 people; the trust level increases from 0.68 for a network of 1500 people to 0.90 for a network of 5000 people.
In this paragraph, we analyze Fig. 3 (i–v). From (i)–(v) of Fig. 3, we show that requirements for trust levels increase for the same individuals in one’s network once the network size increases. From (i) of Fig. 3, to maintain trust among the same five individuals, trust levels require 0.97 and 0.99 once the network size increases to 150 and 500 individuals, respectively. Similarly, to maintain trust among the same 15 individuals, trust levels require 0.90 and 0.97 once the network size increases to 150 and 500 individuals, respectively. Again from (iii) of Fig. 3, to maintain trust among the same 50 individuals, trust levels require 0.66 and 0.90 once the network size increases to 150 and 500 individuals, respectively. However, the trust levels reach 1 asymptotically if the network size increases to ~5000 individuals. In order to maintain trust among the same 150 individuals, the trust level increases from 0.70 for a network of 500 individuals to 0.90 for a network of 1500 individuals. Although one cannot maintain stable relationships with more
than 150 individuals, an increase in trust level is observed in (v) of Fig. 2. Thus, (i)–(v) of Fig. 3 conclude that the requirement for the increase of trust levels among the same individuals in one’s social network increases if the size of the network increases. We are not sure about conspiracies in one’s social network, but we hope that this increase in trust levels as well as the increase in network sizes may be a crucial reason to study various factors of several types of conspiracies or deceptions against one by the individuals in his social network.

In this paragraph, we analyze Fig. 4 (i–viii). From (i) and (ii) of Fig. 4, if \( \alpha = 2.1 \) and \( R_{t=0} = 1 \) for a network of size \( N = 150 \), then the trust cutoff is \( \sim 0.235 \) to reach 50 individuals for both diffusion rates \( \beta = 0.25 \) and \( \beta = 0.50 \) to reach 50 individuals. Similarly, from (iii) and (iv) of Fig. 4, if \( N = 500 \), then the trust cutoff is \( \sim 0.26 \) to reach 150 individuals for \( \beta = 0.25 \) and \( \beta = 0.50 \). For (v) and (vi) of Fig. 4, if \( N = 1500 \), then the trust cutoff is \( \sim 0.50 \) to reach 150 individuals for \( \beta = 0.25 \) and \( \beta = 0.50 \). Again, for (vii) and (viii) of Fig. 4, if \( N = 5000 \), then the trust cutoff is \( \sim 0.79 \) to reach 150 individuals for \( \beta = 0.25 \) and \( \beta = 0.50 \). Thus, trust levels for the same 150 individuals increase with respect to an increase in the size of the network, independent of diffusion rate. Therefore, one cannot expect that information will be shared by the same individuals if his network size increases.

Now, we turn our attention to the power-law distribution of trust. For this purpose, we analyze Fig. 5 (i–iv). At the time of variations in the number of total informed people in one’s network with size \( N = 150 \), the trust cutoff increases to reach 50 individuals in (i) of Fig. 5 with a decrease in the value of the power-law exponent \( \alpha \), where \( 2 < \alpha < 3 \). In (i) of Fig. 5, trust cutoffs are 0.175 and 0.240 for \( \alpha = 2.9 \) and \( \alpha = 2.1 \) respectively. Similar results can be observed for reaching 150 individuals for the same values of power-law exponents in (ii), (iii) and (iv) of Fig. 5 but with different sizes of networks. As observed from the simulations, we can infer that the trust cutoffs increase with a decrease in the power-law exponents \( \alpha \), i.e., \( \alpha \propto 1/(\text{trust cutoff}) \). Thus, we have the following conjecture from the above discussions.

Conjecture: Conspiracies or deceptions are caused in one’s social network if he doesn’t increase his levels of trust for the individuals in his network once the size of the network increases.

5. Comparison with online scenarios in Facebook

This section validates some of our above findings to recent experimental results related to Facebook. It is well-known that Facebook is an influential online social network. Barabási and Albert [3] showed that preferential attachment and growth play important roles to increase the sizes of the real world networks. Moreover, analysis of Facebook was done to detect community structure using 500 million users of Facebook in 2011 by Ferrara [63,64]. In 2012, Ferrara [63,64] showed the existence of power-law distribution for an emerging, well-defined community structure inside Facebook. Since, power-law exponent, i.e., \( \alpha \) exhibits the existence of hubs (of higher connections) in any real life network, thus obviously Facebook is one of the most suitable online social networks to validate our theoretical claims of previous section. Hence, \( \alpha \), i.e., power-law exponent has several strong implications on Facebook. Using the same simulations as in the previous section, we have similar conclusions for the 500 million Facebook users [63,64]. We also found that

---

**Fig. 5.** The power-law distribution having (i) trust cutoffs with \( \alpha = 2.1 \) to 2.9 when \( N = 150 \), (ii) trust cutoffs with \( \alpha = 2.1 \) to 2.9 when \( N = 500 \), (iii) trust cutoffs with \( \alpha = 2.1 \) to 2.9 when \( N = 1500 \), (iv) trust cutoffs with \( \alpha = 2.1 \) to 2.9 when \( N = 5000 \).
there is a requirement for trust levels to increase among the same individuals in one’s social network if the size of the network increases to 500 million users of Facebook. As a relation between the power-law exponent $\alpha$ and the trust cutoff, it is found that $\alpha \propto 1/(\text{trust cutoff})$. Moreover, we also find that trust levels never help to diffuse information quickly or vice versa to reach Dunbar’s number 150, along with hierarchy layers of 5, 15, and 50 individuals in networks of different sizes. We provide Fig. 6 (i-ii) for the verification of our first conclusion of the previous section in case of 500 million users of Facebook. One can also obtain remaining conclusions of the previous section by using the same simulations for $N = 500$ million user of Facebook.

In 2014, Kraut and Foire [65] surveyed 472,231 online groups on Facebook to find out about their success and survival. They found that 57% of these groups ceased to create new content by the end of three months. Groups were found to be less likely to survive when the founders had more ties to group members, when the founders invited more of the members, and when the founders served as exclusive administrators of the group. Moreover, larger groups that engaged founders vigorously in the first week of their formation were found to be more successful than smaller and less engaging groups. Similar to above, Ma et al. [66] surveyed on 6383 users of Facebook groups about their trust attitudes. Following aggregated behavioral and demographic data for group members, they concluded that (1) an individual’s propensity to trust is associated with how they trust their groups, (2) groups that are smaller, closed, older, more exclusive, or more homogeneous are trusted more; and (3) trust can be predicted from a group’s overall friendship-network structure and an individual’s position within the structure. In Ref. [66], Ma et al. also found that trust decreases with the increase of the group size. But interestingly, they confirmed the finding of Kraut and Foire [65] that trust grows with the number of group administrators. They also suggested that less popular groups should be recommended to individuals because of the diversity of group recommendations, trust, and user satisfaction. Ma et al. [66] did not find any significant difference between closed and secret groups once the groups’ sizes crossed Dunbar’s number 150. Moreover, Cohen and Havlin [67] and Guardiola et al. [68] found that trust cooperation networks possess scale-free degree distributions. Since, power-law exponent $\alpha$ has major roles in scale-free degree distributions, thus combining results from Refs. [63-67] it can be understood that our result $\alpha \propto 1/(\text{trust cutoff})$ may have a significant impact on online and offline social networks. Again, preferential attachments are present in scale-free networks [3,69], so it can be found that the number of individuals with lower trust cutoffs in an individual’s social network increases if the size of his social network grows. So, the trust cutoff is not absolute in social networks. Hence, one must increase trust cutoffs for individuals in his social network if he doesn’t want to be deceived by members of his social network due to the increase in its size. Thus, we have found that one of our predictions is matched to one of the data based observations related to trust and the size of social networks made by Ma et al. [66]. Thus, we hope to have more rigorous data based results to validate our claims.

6. Limitations and scopes of further research

In the case of one’s social network, we showed that $\alpha \propto 1/(\text{trust cutoff})$. To validate our theoretical claims, we considered some related studies on Facebook and trust. However, like Facebook, analyses of networks on Twitter also confirmed Dunbar’s number as the cognitive limit of Twitter users [70]. Recently Lu et al. [71] analyzed 50000 tweets from April 30 to May 30 of 2013. A total of 42180 participants were covered in this analysis. They concluded that the frequency distribution of retweeting is described by a power-law, with $\alpha$ ranges from 0.6 to 0.7. Similarly, Aparicio et al. [72] also confirmed power-law distribution in the case of Twitter. Hentschel et al. [73] identified trust worthy users on Twitter. But, no such analysis on Twitter, best to our knowledge, has been done so far like Facebook [65,66]. Thus, it limits us to validate our results on social networks like Twitter at present. Thus, we hope to have suitable experimental validations of our results for Twitter and other social networks in future.

7. Conclusion

In this paper, we tried to find out how various types of trust distributions like uniform and power-law in a network result in information diffusion, as well as how the changes in the sizes of the networks make a difference in the trust level of individuals to keep the same number of friends in each hierarchy. We found that trust levels remain the same irrespective of the information diffusion rate in a network. It means that trust level never helps to diffuse information quickly or vice versa to reach Dunbar’s number 150 along with hierarchy layers of 5, 15, and 50 individuals in networks of different sizes. Moreover, the requirement for trust levels among the same individuals in one’s social network increases if the size of his social network increases. Also, trust levels for the same 150 individuals increase with respect to an increase in the size of the network, independent of diffusion rate. Therefore, one cannot expect that information will be shared by the same individuals if his network size increases. We can infer that the trust cutoffs increase with a decrease in the power-law exponents, i.e., $\alpha \propto 1/(\text{trust cutoff})$. However, we are not sure whether conspiracies or deceptions are caused in one’s social network if he doesn’t increase his levels of trust in individuals in his social network once the size of his social network increases. Thus, we proposed it as a conjecture to the readers for validation. Moreover, we hope that to find topological connections [74,75] of this paper in social networks in future.

8. Open questions

In this section, we propose the following questions that are open in the common research domain of social networks, Dunbar’s number, and trust.

Q.1. What are the topological and graph theoretical features of one’s social network in terms of centrality, connectivity, etc. If trust levels are increased among members of the network?

Q.2. Are there hidden mathematical and social network patterns in wars that were/are caused by deception?
Author contribution statement

Santanu Acharjee: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Wrote the paper.
Akhil Thomas Panicker: Performed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Data availability statement

No data was used for the research described in the article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was supported in part by the International Centre for Theoretical Sciences (ICTS) during the participation of both the authors for participating in the program-Summer research program on Dynamics of Complex Systems (Code: ICTS/Prog-DCS2019/07). The authors are thankful to Prof. Robin I. M. Dunbar of the University of Oxford for his constructive discussions during the preparation of this paper.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.heliyon.2023.e19850.

References

[1] J.A. Barnes, Graph theory and social networks: a technical comment on connectedness and connectivity, Sociology 3 (2) (1969) 215–232.
[2] P. Erdös, A. Rényi, On the evolution of random graphs, Publ. Math. Inst. Hungar. Acad. Sci. 5 (1960) 17–61.
[3] A.L. Barabasi, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[4] J.A. Barnes, F. Harary, Graph theory in network analysis, Soc. Netw. 5 (2) (1983) 235–244.
[5] P. Hage, F. Harary, Eccentricity and centrality in networks, Soc. Netw. 17 (1) (1995) 57–63.
[6] P.N. Hsiao, A social network model based on topology vision, in: J. Zhou (Ed.), Complex Sciences, Complex 2009, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 5, Springer, Berlin, Heidelberg, 2009.
[7] S. Salem, S. Banitaan, I. Aljarah, J.E. Brewer, R. Alroobi, Discovering communities in social networks using topology and attributes, Proceedings of 10th International Conference on Machine Learning and Applications 1 (2011) 40–43.
[8] K.S.K. Chung, M. Piraveenan, L. Hossain, Topology of online social networks, in: R. Alhajj, J. Rokne (Eds.), Encyclopedia of Social Network Analysis and Mining, Springer, New York, 2014.
[9] K. Juszczyszyn, P. Kazienko, K. Musial, Local topology of social network based on motif analysis, in: I. Lovrek, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems. KES 2008. Lecture Notes in Computer Science, vol. 5178, Springer, Berlin, Heidelberg, 2008.
[10] E. Ferrara, G. Fiumara, Topological features of online social networks, Commun. Appl. Ind. Math. (2012) 20, https://doi.org/10.1685/journal.caim.381.
[11] M.C. Waunmus, T. Nicodème, H. Bersini, Topology analysis of social networks extracted from literature, PLoS One 6 (10) (2011), e19465.

[12] M. G. F. Pansieri, E.F. Pavone, A. Merla, S.M. Aglioti, Situational and dispositional determinants of intentional deceiving, PLoS One 6 (4) (2011), e19465.

[13] F. Gino, S. Ayal, T. Ariely, Self-serving altruism? The lure of unethical actions that benefit others, J. Econ. Beh. Org. 93 (2013) 285–299.

[14] J. T. Hancock, J. Thom-Santeli, T. Ritchie, Deception and design: the impact of communication technology on lying behavior, CHI Lett 6 (2004) 130.

[15] B. DePaulo, D. Kashy, S. Kirkendol, M. Wyer, J. Epstein, Lying in everyday life, J. Pers. Soc. Psychol. 70 (1996) 979–999.

[16] R. Falcone, C. Castelfranchi, Social trust: a cognitive approach, in: C. Castelfranchi, Y. Tan (Eds.), Trust and Deception in Virtual Societies, Kluwer Academic Publishers, Boston, 2001, pp. 55–92.

[17] R. Falcone, C. Castelfranchi, The socio-cognitive dynamics of trust: does trust create trust? in: R. Falcone, et al. (Eds.), Trust in Cybernetworks: Integrating the Human and Artificial Perspectives Springer, Berlin, 2001, pp. 55–92.

[18] M.A. Nowak, K. Sigmund, Evolution of indirect reciprocity, Nature 437 (2005) 1291–1298.

[19] R.I.M. Dunbar, Constraints on the evolution of social institutions and their implications for information flow, J. Inst. Econ. 7 (3) (2011) 345–464.

[20] J.B. Rotter, Generalized expectancies for interpersonal trust, Amer. Psy 26 (5) (1971) 443–452.

[21] A. S. Milgram, T. Travers, A. Vespignani, Modeling users activity in social networks, Sci. Rep. 3 (2013) 1873.

[22] N. Memon, R. Alhajj (Eds.), From Sociology to Computing in Social Networks, Springer, Vienna, 2010.

[23] J. Bentham, An Introduction to the Principles of Morals and Legislation, Clarendon Press, Oxford, 1789.

[24] S. B. Hays, R. Duschnak, J. Binder, H. Arrow, Relationships and the social brain: integrating psychological and evolutionary perspectives, Br. J. Psychiatry 103 (2012) 149–168.

[25] S.G.B. Roberts, C. Ronwick, The Development of Cooperative Relationships: an Experiment, vol. 270, Proc. Royal Soc. London, 2003, pp. 2279–2283.

[26] S. Usai, R. Alhajj, Social networks: a powerful model for serving a wide range of domains, in: N. Memon, R. Alhajj (Eds.), From Sociology to Computing in Social Networks, Springer, Vienna, 2010.
[73] M. Hentschel, O. Alonso, S. Counts, V. Kandylas, Finding users we trust: scaling up verified Twitter users using their communication patterns, Proceedings of the International AAAI Conference on Web and Social Media 8 (1) (2014) 591–594.

[74] J.W. Berry, C.A. Phillips, J. Saia, Making social networks more human: a topological approach, Stat. Anal. Data Min. 12 (6) (2019) 449–464.

[75] E. Mossel, A. Sly, O. Tamuz, Strategic learning and the topology of social networks, Econometrica 83 (5) (2015) 1755–1794.