Modeling the Impact of Privacy on Information Diffusion in Social Networks

Modeling the Impact of Privacy on Information Diffusion in Social Networks

Livio Bioglio and Ruggero G. Pensa

University of Turin - Dept. of Computer Science, Turin, Italy
{livio.bioglio,ruggero.pensa}@unito.it

Abstract. Humans like to disseminate ideas and news, as proved by the huge success of online social networking platforms such as Facebook or Twitter. On the other hand, these platforms have emphasized the dark side of information spreading, such as the diffusion of private facts and rumors in the society. Fortunately, in some cases, online social network users can set a level of privacy and decide to whom to show their information. However, they cannot control how their friends will use this information. The behavior of each user depends on her attitude toward privacy, that has a crucial role in the way information propagates across the network. With the aim of providing a mathematical tool for measuring the exposure of networks to privacy leakage risks, we extend the classic Susceptible-Infectious-Recovered (SIR) epidemic model in order to take the privacy attitude of users into account. We leverage such model to measure the contribution of the privacy attitude of each individual to the robustness of the whole network to the spread of personal information, depending on its structure and degree distribution. We study experimentally our model by means of stochastic simulations on four synthetic networks generated with classical algorithms.

Keywords: complex networks, modeling, information diffusion, privacy

1 Introduction

Humans are social animals that love to disseminate ideas and news, as proved by the huge success of social networking websites such as Facebook or Twitter. On the other hand, these platforms have emphasized the dark side of information spreading such as the diffusion of private facts and rumors that may additionally foster slander and cyberbullying acts [21]. As a consequence, the users of online social networks are acquiring a new awareness of the importance of their own privacy on the Web. However, although most users do not disclose very sensitive facts (private life events, diseases, political ideas, sexual preferences, and so on), they are simply not aware of the risks due to the disclosure of less sensitive information, such as GPS tags, photos taken during a vacation period, page likes, or comments on news. Some social media provide advanced tools for controlling the privacy settings of the user's profile [26]. However, yet a large part of Facebook content is shared with the default privacy settings and exposed to more users than expected [17]. According to Facebook CTO Bret Taylor, even though most people have modified their privacy settings[1], in 2012, still “13 million users [in the United States] said they had never set, or didn’t know about, Facebook’s privacy tools[2]”. Moreover, even though the users of these social networks can usually set a level of privacy, and specify which of their contacts are allowed to see their notifications, they do not have any control on how these contacts will use the information: friends could spread the rumor through other social networks, blogs, websites, medias or simply with face-to-face communication.

The behavior of an individual in these situations highly depends on her level of privacy awareness: an aware user tends not to share her private information, or the private information of her friends on social networks, while an unaware user could not recognize an information as private, and could share it without care to her contacts, even to untrusted ones, putting at risk her privacy or the privacy of her friends. Users’ privacy awareness then turns into the so-called “privacy attitude”, i.e., the users’ willingness to disclose their own personal data to other users, that can be measured by leveraging the way users customize their privacy settings in social networking platforms [16, 24].

The privacy attitude of each actor in a social network heavily influences the effects of information propagation, not only for posts that are clearly private [30]. In fact, it is a well-known fact that by leveraging Facebook user’s activity (such as ”Likes” to posts or fan pages) it is possible to “guess” some very private traits of the user’s personality [15]. For instance, a public comment on news posts may reveal the political ideas of the individual. However, the privacy attitude alone is not a good measure of the user’s objective privacy leakage, since the latter depends also on other users’ attitude to privacy and the way they contribute in the information propagation process. With the aim of providing a mathematical tool for measuring the exposure of networks to privacy leakage risks, in this paper we study the effects of privacy attitude on information propagation by extending the classic Susceptible-Infectious-Recovered (SIR) epidemic model. In this model, an individual may be susceptible, infectious or recovered: a susceptible individual in contact with an infectious one can become infectious with a transmission probability, while an infectious individual naturally recovers from infection with a recovery rate, turning into a recovered individual. The SIR model can be adopted for modeling the spread of information in a social network [12]: susceptible individuals do not know the information, then are susceptible to be informed; infectious individuals know and spread the information, while recovered individuals already know the information but do not spread it anymore. We extend this compartmental model in order to represent privacy attitude. In our model, each individual belongs to a privacy attitude class that tunes the parameters of the model. The privacy attitude of users has an influence on the way information spreads across the network that additionally unveil its realis-

[1] http://www.zdnet.com/article/facebook-cto-most-people-have-modified-their-privacy-settings/

[2] http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm

tic robustness to information leakage as the effects of information propagation within this model. We use our model, by means of stochastic simulations, for studying the role of privacy on the information diffusion in several synthetic networks, generated from classic algorithms, with different distributions of attitude on privacy of their nodes.

The remainder of the paper is organized as follows: we briefly review the related literature in Section 2; the privacy-aware propagation model is presented in Section 3; Section 4 provides the report of our experimental research; Section 5 shows how to infer the privacy attitude of a social network user from her profile settings; finally, we draw some conclusions in Section 6.

2 Related work

In epidemiology, the Susceptible-Infectious-Recovered (SIR) epidemic model [13] is employed for modeling infectious diseases that confer lifelong (or long-term) immunity, such as measles, rubella or chickenpox. In this model a susceptible node can become infected, because of the presence of infectious nodes, and an infectious node can naturally recover after few time, gaining immunity to the disease.

The SIR model has been applied to information spreading since early years, even if these applications slightly differ from the common model: in [9] when a spreader meets another infectious node, that already knows the rumor, both lose interest in spreading it any further, and become recovered, while in [18] when two infectious nodes meet, only one node turns into recovered, and the other one remains unchanged. This last version of SIR model for rumor spreading has been widely studied: in [22] the author found that in a complete random network, i.e., a homogeneous network, a rumor can only spread to around the 80% of the total population; more recently in [27] it has been calculated that such percentage is lower than 80% in small-world networks. In [29] the authors found that the number of nodes reached by the rumor depends on the topological structure of the network, decreasing when it changes from random to scale-free network, and on the mean degree of the network, increasing when the mean degree increases; the same happens for the probability of a single node to be informed, that increases when the degree of node increases. Such behavior happens because large hubs are rapidly reached by the rumor, but they easily turn into recovered, preventing the spreading of the rumor to their huge neighborhood. This is confirmed by the observation, in [19], that the density of susceptible nodes at the end of the process decays exponentially with the value of their degree. An extension of this model also allows spontaneous recovery, justified as forgetting mechanism: an infectious node should also turn into recovered spontaneously after a random time. In this case, the model behave more similarly to the classical SIR model, as observed in [20].

In our work, we focus on rumor spreading in presence of a sort of "immunization parameter" that models the privacy attitude of users, i.e., their willingness to disclose their own personal data to other users directly or indirectly. At the best of our knowledge, this is the first attempt of modeling and measuring the robustness of networks to privacy leakage risks by means of a classic epidemic models in social networks. Indeed, a large part of research works on privacy issues in online social networks focus on the anonymization of networked data [28]. Differently from those studies, our work can be positioned in another branch of research that focuses on modeling, measuring and preventing privacy leakage in online social networks. In this regard, one of the most prominent work is [16] where Liu and Terzi propose a framework to compute a privacy score measuring the users' potential risk caused by their participation in the network. This score takes into account the sensitivity and the visibility of the disclosed information and leverages the item response theory as theoretical basis for the mathematical formulation of the score. In [24], the authors define a privacy index that leverages the privacy settings of users to measure their privacy exposure in an online social network according to predefined sensitivity values for users' items. [7] presents a tool to detect unintended information loss in online social networks by quantifying the privacy risk attributed to friend relationships in Facebook. The authors show that a majority of users' personal attributes can be inferred from social circles. In [23] the authors measure the inference probability of sensitive attributes from friendship links. In [3, 2], the authors define a measure of how much it might be risky to have interactions with them, in terms of disclosure of private information. Among all these research contributions, [16] is the only one that also consider the privacy attitude of users in disclosing their personal data and provide a mathematical formulation for it. This formal definition can be used to tune our information-propagation model according to the attitude towards privacy of the users involved in the social network.

3 A privacy-aware model for information spreading

In this section, we introduce the the Susceptible-Infectious-Recovered (SIR) epidemic model for modeling the contribution of privacy on information spreading in a social network. Before providing the details of our privacy-aware information-propagation model, we introduce the notation required to formalize the problem.

We consider a social graph G involving a set of n vertices $\{v_1, \dots, v_n\}$ that are the users participating in G. In this work, the social network is then a represented as a directed graph $G(V, E)$, where V is a set of n vertices and E is a set of directed edges $E = \{(v_i, v_j)\}$. Given a pair of vertices $v_i, v_j \in U$, $(v_i, v_j) \in E$ iif there exists a link from v_i to v_j (e.g., users v_i is in the friend list/circle of v_j or v_j follows v_i). For any given vertex $v_i \in V$ we define the neighborhood $\mathcal{N}(v_i)$ as the set of vertices v_k which vertex v_i is directly connected to, i.e., $\mathcal{N}(v_i) = \{v_k \in V \mid (v_i, v_k) \in E\}$. Conversationally speaking, $\mathcal{N}(v_i)$ is the set of followers of user v_i. Furthermore, we assume that each user v_i belongs to a privacy class $p \in P$, which is defined as the propensity of an user of the class to disclose her own or other's personal information, directly or indirectly. In practical terms, in online social networks (such as Facebook, Twitter, Instagram

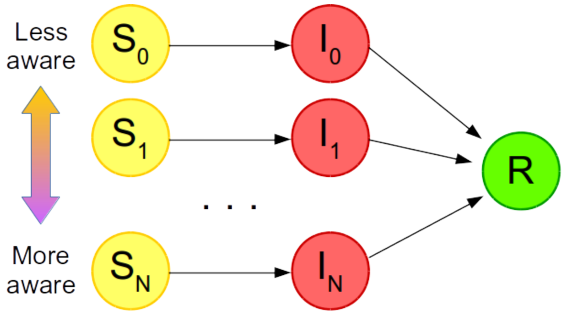

Fig. 1. Transmission model. Each index of compartments S and I represents a privacy class

or Google+) the privacy class may be unveiled by the way users configure their privacy settings, or the way they post or share/comment other users' posts.

3.1 Information spreading model

In the SIR model, at any time step an individual v_i belongs to one compartment among susceptible (S), infectious (I) and recovered (R). An infectious (I) individual v_i may spontaneously recovers from infection with a probability μ, called recovery probability, entering the recovered (R) compartment, or it may spread the disease to a susceptible (S) individual with which it is in contact with a probability λ, called infection probability: the infected susceptible (S) individual immediately becomes infectious (I). We denote with $c(v_i, t) \in \{S, I, R\}$ the compartment of user v_i at time t.

The SIR model can be also applied for the spread of information in a population: susceptible individuals are those who not already know the information, and then they are susceptible to be informed; infectious individuals know the information and actively spread it; finally, recovered individuals are the ones who know the information but do not spread it anymore. The recovery process models a mechanism of aging of the information, that after few time loses its interest or its novelty for an individual and stops to be spread by him. In our formulation, the population is the set of n users $V = \{v_1, \ldots, v_n\}$, while the information may only spread from a user v_i to a user v_j if there exists an edge (v_i, v_j) connecting v_i to v_j[3].

Here we propose an extension of this model that takes into account the explicit or implicit privacy policies of individuals during the spread of information. A set of privacy classes $P = \{p_0, p_1, \ldots, p_N\}$ is assigned to Susceptible and Infectious compartments, representing the privacy class of an individual belonging to the compartment, and consequently her behavior on information spreading, from less aware (p_0) to more aware (p_N). A graphic representation of our model

[3] Thus, in our model, the edges are directed from the source of the information to its target.

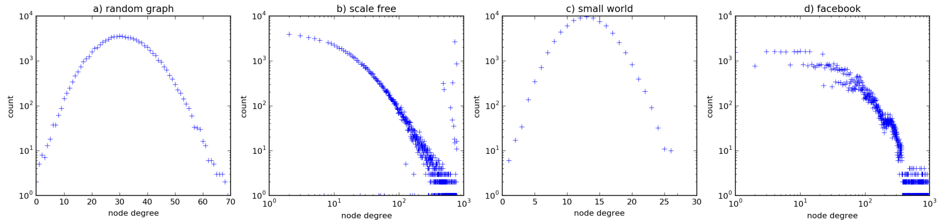

Fig. 2. Degree distribution for each synthetic network

is given in Figure 1. Moreover we insert a novel parameter $\beta_p \in [0, 1]$ to the SIR transmission model, that is the interest of users in privacy class p in information. Each privacy class differs for the values assigned to the three parameters (β, λ and μ) of the transmission model. Hence, given the privacy class p, parameters β_p, λ_p and μ_p are completely defined.

The evolution of the spread follows the Reed-Frost chain-binomial model [1]: it consists in a stochastic approach, where time is measured in discrete units and infection occurs because of direct contacts. The evolution probabilities are obtained as follows. Let $p(v_i) = p \in P$ be the privacy class of an individual v_i. If it belongs to the susceptible compartment, it may be infected at time $t + 1$ with probability:

$$P_{inf}(v_i, t+1) = \beta_p \cdot (1 - \prod_{p' \in P} (1 - \lambda_{p'})^{n_I(v_j,t)}) \tag{1}$$

where $n_I(v_j, t) = |\{v_j \in \mathcal{N}(v_i) \mid c(v_j, t) = I \ \wedge \ p(v_j) = p'\}|$ is the number of individuals in compartment I (infectious) and privacy class p' at time t among the neighbors of individual v_i. Otherwise, if the individual v_i of privacy class p belongs to the infectious compartment I at time t, it may recover with probability μ_p at time $t + 1$.

4 Experiments and results

In this section we provide the results of our experiments performed over several types of synthetic networks. In a nutshell, we generate four networks, each one with a different structure and degree distribution. On each one, we observe the number of nodes reached by the information for three different assignments of privacy classes to the nodes, representing the global attitude on privacy of the network.

4.1 Contact networks

The information spreads on a contact network, in which nodes represent individuals, and edges between nodes represent contacts between two individuals. Since our objective is to study and characterize the dynamic behavior of the model,

Table 1. Values of the parameters for the three privacy classes

	Classes		
Parameter	0	1	2
β	0.9	0.5	0.1
μ	0.1	0.3	0.5
λ	0.9	0.5	0.1

here we employ four types of networks, generated with standard algorithms. In all networks, the links between nodes are always considered as reciprocal, i.e., all the graph considered in these experiments are undirected.

The four synthetic networks have approximately the same number of nodes, 75,000, and the same number of edges, around 2,700,000. The first synthetic network is a random graph, also known as an Erdös-Rényi graph [10], generated by means of the fast algorithm in [6]. The second one is a scale-free graph generated with the Barabasi-Albert algorithm [4] where new nodes are attached with 36 edges to existing nodes with high degree. The third one is a small-world network generated through the Watts-Strogatz mechanism [25] where each node is joined with its 72 nearest neighbors in a ring topology, and each edge has a probability of rewiring equal to 0.15. The fourth one is a Facebook-like network generated using LDBC–SNB Data Generator[4] which produces graphs that mimic the characteristics of real Facebook networks [11]: in particular, we generate a network with 80,000 nodes, but here we consider only the greatest connected component of such network. The degree distributions of these networks are given in Figure 2

4.2 Privacy class distributions

In our experiments, we select three privacy classes, numbered from 0 to 2, representing users from unaware (class 0) to more aware on privacy (class 2), in order to provide a few grades of awareness. The values assigned to the parameters of the information spreading model for each class are reported in Table 1. Users in class 0 have a high probability of being interested in information and spreading it over the network for a long period of time ($1/\mu$ is the average duration of the infection). On the contrary, users in class 2 have a very low probability of being interested in information: even if they are reached by information, they spread it only for few time steps. Consequently, the probability of diffusing the information is very low for such users. Finally, class 1 represents average users, then its parameters have been tuned accordingly.

For each network in Section 4.1, we randomly assign to each node a privacy class, according to three probability distributions: a safer assignment, where the majority of nodes are in class 2, the most aware one; a medium assignment, where the majority of nodes are in class 1; an unsafer assignment, where the majority of nodes are in the less aware class 0. The number of nodes in each

[4] `https://github.com/ldbc/ldbc_snb_datagen`

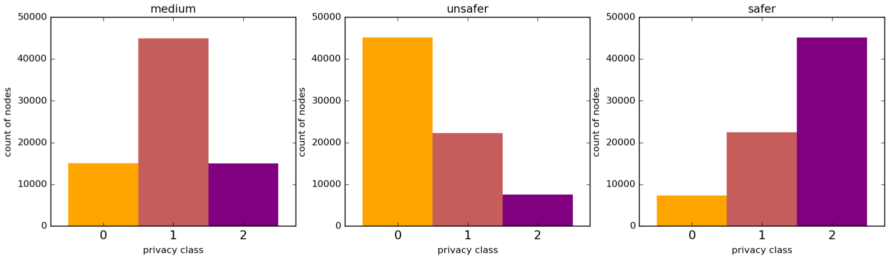

Fig. 3. Class distribution in the three kinds of class assignments

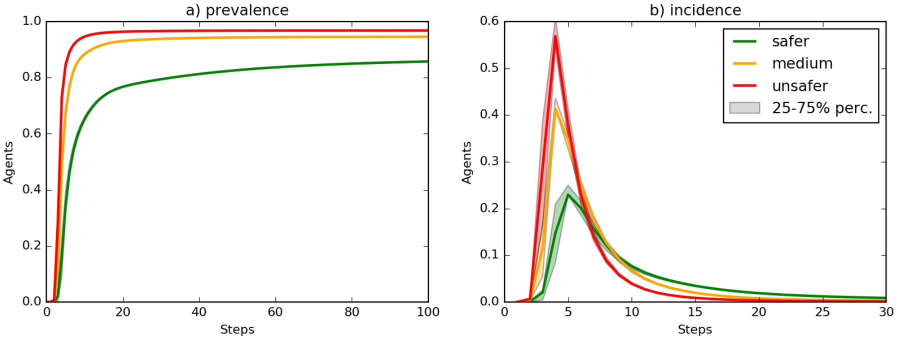

Fig. 4. Prevalence and incidence of informed individuals (ratio) in the scale-free network for each class distribution

privacy class of these three class distributions are graphically summarized in Figure 3.

4.3 Experimental settings

Our experiments are conducted as follows. For each contact network in Section 4.1, and for each class distribution in Section 4.2, we perform 100 stochastic simulations of information spreading on a completely susceptible population, except for one infectious node. These simulations are repeated for 9 different initial spreaders, randomly chosen among all the nodes, 3 for each privacy class. For each set of simulations we observe the number of informed individuals over time, that is the number of nodes in compartments infectious or recovered, and we calculate the proportion of cases at each time step (prevalence) and the proportion of new cases at each time step (incidence). The results on the same network and class distribution are aggregated.

4.4 Results

We study the impact of the distribution of individuals having different awareness on privacy on the spread of an information in all the synthetic networks described

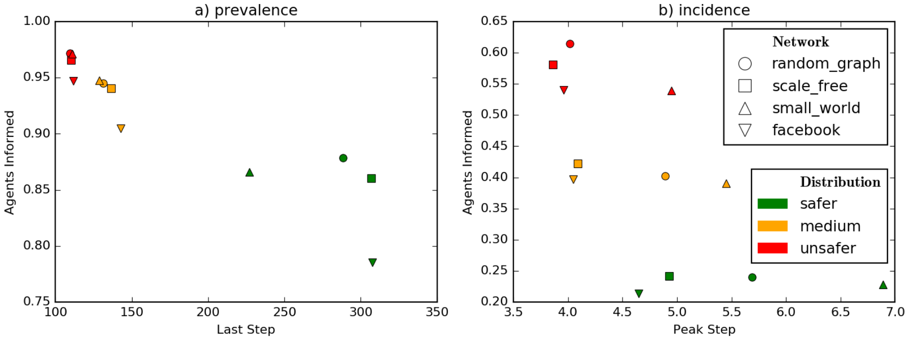

Fig. 5. Prevalence and incidence of informed individuals (ratio) in each network model and class distribution

in Section 4.1. Figure 4 shows our results for the scale-free network. From the curves of prevalence in Figure 4(a) we can notice that the number of informed individuals over time greatly depends on the distribution of privacy classes of the network: where the majority of node is unaware, the information immediately spreads over almost the entire population, while where the network is full of aware individuals the information spreads slowly, and reaches a smaller part of the population. The speed of diffusion is more evident in the curves of incidences, in Figure 4(b), which depicts the proportion of new cases of informed individuals in each time step: under the least safe distribution, the information immediately reaches more than half of population, while for safer distributions this peak is lower, and it is reached few steps later.

In order to compare the behavior of all networks in Section 4.1, we collect some key features of the prevalence and the incidence curves: for the prevalence ones, we collect the proportion of informed individuals at the end of simulations, that is when there are no more infectious individuals who can spread information, and the step where simulation ends, in order to obtain the duration of the spread and its diffusion among the population; for the incidence curves, we collect the information on the peak of new cases of informed individuals, and the step where the peak is reached, for obtaining a snapshot of the speed of the diffusion of information. These data for all the networks are graphically summarized in Figure 5.

We can notice that the behavior observed for random graph network happens similarly for all the other networks. Under the safest class distribution, the information reaches a smaller proportion of the population. Furthermore, it stops to be diffused much later than in less safer distributions. Interestingly, even in case of safer distribution an information reaches a huge portion of the population, and such proportion is always smaller for the Facebook-like network: apparently such kind of network is the worst one for spreading an information, especially in case of safer class distribution. As regards the diffusion speed, the small-world network is the last one reaching the peak, while on the other side the

Facebook-like network is the faster one. However, even if the peak value is really different among the distributions, the steps where peak is reached are not so far: in any case an information reaches almost immediately the maximum number of uninformed individuals. It is worth noting that the contribution of privacy attitude on incidence is significant: this means that this parameter should be taken into account in viral campaigns where the goal is to maximize the number of informed nodes in the shortest possible time. On the other hand, the substantial differences given by the network structure and their degree distribution cannot be ignored when measuring the privacy leakage risk of users.

5 Privacy attitude estimation

In Section 3 we have created privacy classes, tuning the characteristic parameters of propagation model, according to the privacy attitude of users. Such attitude, however, involves several psychological, cultural and contextual factors, and it may be indeed difficult to model in real cybersocial systems. In this section we briefly show how to infer it for generic users using some information about their profile settings or disclosing behavior[5]. Our attitude estimation, inspired by the framework defined by Liu and Terzi [16], measures the user's potential risk caused by her participation in the network by assigning to each user a privacy score according to her privacy settings. A $n \times m$ response matrix $\boldsymbol{R}$ is associated to the set of n users and a set of m profile items (e.g., age, gender, education, political views, and so on). Each element r_{ij} of $\boldsymbol{R}$ contains a privacy level that determines the willingness of user i to disclose information associated with profile item j. In [16], the Item Response Theory (IRT) model is adopted to measure the privacy attitude of the users, the sensitivity of the questions, and the probability of a user deciding a given level of visibility to a given profile property. In a binomial case, the probability that a user i sets item j visible to everyone is computed as:

$$P_{ij} = Prob\{r_{ij} = 1\} = \frac{1}{1 + e^{-\alpha_j(\theta_i - \sigma_j)}} \tag{2}$$

where α_j is the discrimination power of item j, σ_j is the sensitivity of j and θ_i is the privacy attitude of user i. In [16], the authors provide an Expectation-Maximization algorithm to estimate parameters α_j and σ_j by only leveraging the response matrix $\boldsymbol{R}$.

When parameters σ_j and α_j ($\forall j \in \{1 \ldots m\}$) are known, each θ_i can be computed by maximizing the following log-likelihood function:

$$L = \sum_{j=1}^{m} [r_{ij} \log P_{ij} + (1 - r_{ij}) \log (1 - P_{ij})] \tag{3}$$

derived from the likelihood $\prod_{k=1}^{m} P_{ij}^{r_{ij}} (1 - P_{ij})^{1 - r_{ij}}$. The solutions can be computed using the Newton-Raphson method, an iterative algorithm that estimates the value of θ_i at iteration t starting from the value of θ_i at iteration $t - 1$ [16].

[5] Such information is known by social network providers.

6 Conclusions

In this paper we have proposed an information propagation model that considers the role of privacy awareness on information spreading inspired by the classical SIR epidemic model. We have assigned different privacy classes to the nodes of networks, depending on their attitude on privacy, in order to model populations more or less interested on diffusing an information. Through stochastic simulations we have studied the impact of the attitude on privacy of a connected population on the proportion of individuals reached by an information diffused by an unique spreader on a random, a scale-free, a small-world and Facebook-like network.

Our results show that the attitude on privacy can really have an impact on the diffusion of an information, by reducing or increasing the portion of population which receives the information according to safer or less aware attitude on privacy of the individuals on the network. The same behavior happens in all the structures under study, but the Facebook-like network seems to be the most robust to information diffusion.

Our study shows the importance of considering privacy attitude of users in modeling the spreading of rumors, with direct and indirect implications on all applications that involve the dynamics of information spreading, such as influence maximization [14] and community detection [5], as well as on privacy enforcement models and techniques for online social networks, thus inspiring the design of privacy-preserving social networking components for *Privacy by Design* compliant software [8].

Acknowledgments This work was supported by Fondazione CRT (grant number 2015-1638).

References

1. H. Abbey. An Examination of the Reed-Frost Theory of Epidemics. *Human Biology*, 24(3):201, 1952.
2. C. G. Akcora, B. Carminati, and E. Ferrari. Privacy in social networks: How risky is your social graph? In *Proceedings of IEEE ICDE 2012*, pages 9–19. IEEE Computer Society, 2012.
3. C. G. Akcora, B. Carminati, and E. Ferrari. Risks of friendships on social networks. In *Proceedings of IEEE ICDM 2012*, pages 810–815. IEEE Computer Society, 2012.
4. A.-L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.
5. N. Barbieri, F. Bonchi, and G. Manco. Influence-based network-oblivious community detection. In *Proceedings of IEEE ICDM 2013*, pages 955–960. IEEE Computer Society, 2013.
6. V. Batagelj and U. Brandes. Efficient generation of large random networks. *Physcal Review E*, 71, 2005.
7. J. Becker and H. Chen. Measuring privacy risk in online social networks. In *Proceedings of Web 2.0 Security and Privacy (W2SP) 2009*, 2009.

8. A. Cavoukian. Privacy by design [leading edge]. *IEEE Technol. Soc. Mag.*, 31(4):18–19, 2012.
9. D. J. Daley and D. G. Kendall. Epidemics and rumours. *Nature*, 208:1118, 1964.
10. P. Erdös and A. Rényi. On random graphs. *Publicationes Mathematicae*, 6:290–297, 1959.
11. O. Erling, A. Averbuch, J. Larriba-Pey, H. Chafi, A. Gubichev, A. Prat-Pérez, M. Pham, and P. A. Boncz. The LDBC social network benchmark: Interactive workload. In *Proceedings of ACM SIGMOD 2015*, pages 619–630. ACM, 2015.
12. D. Gruhl, D. Liben-Nowell, R. V. Guha, and A. Tomkins. Information diffusion through blogspace. *SIGKDD Explorations*, 6(2):43–52, 2004.
13. M. J. Keeling and P. Rohani. *Modeling Infectious Diseases in Humans and Animals*. Princeton University Press, 2008.
14. D. Kempe, J. M. Kleinberg, and É. Tardos. Maximizing the spread of influence through a social network. In *Proceedings of ACM SIGKDD 2003*, pages 137–146. ACM, 2003.
15. M. Kosinski, D. Stillwell, and T. Graepel. Private traits and attributes are predictable from digital records of human behavior. *PNAS*, 110(15):5802–5805, 2013.
16. K. Liu and E. Terzi. A framework for computing the privacy scores of users in online social networks. *TKDD*, 5(1):6, 2010.
17. Y. Liu, P. K. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of ACM SIGCOMM IMC '11*, pages 61–70. ACM, 2011.
18. D. P. Maki and M. Thompson. *Mathematical models and applications: with emphasis on the social, life, and management sciences*. Prentice-Hall, 1973.
19. Y. Moreno, M. Nekovee, and A. F. Pacheco. Dynamics of rumor spreading in complex networks. *Physical Review E*, 69(6):066130, 2004.
20. M. Nekovee, Y. Moreno, G. Bianconi, and M. Marsili. Theory of rumour spreading in complex social networks. *CoRR*, abs/0807.1458, 2008.
21. R. A. Sabella, J. W. Patchin, and S. Hinduja. Cyberbullying myths and realities. *Computers in Human Behavior*, 29(6):2703–2711, 2013.
22. A. Sudbury. The proportion of the population never hearing a rumour. *Journal of applied probability*, pages 443–446, 1985.
23. N. Talukder, M. Ouzzani, A. K. Elmagarmid, H. Elmeleegy, and M. Yakout. Privometer: Privacy protection in social networks. In *Proceedings of M3SN'10*, pages 266–269. IEEE, 2010.
24. Y. Wang, R. K. Nepali, and J. Nikolai. Social network privacy measurement and simulation. In *Proceedings of ICNC 2014*, pages 802–806. IEEE, 2014.
25. D. J. Watts and S. H. Strogatz. Collective dynamics of'small-world'networks. *Nature*, 393(6684):409–10, 1998.
26. L. Wu, M. Majedi, K. Ghazinour, and K. Barker. Analysis of social networking privacy policies. In *Proceedings of 2010 EDBT/ICDT Workshops*. ACM, 2010.
27. D. H. Zanette. Dynamics of rumor propagation on small-world networks. *Physical review E*, 65(4):041908, 2002.
28. E. Zheleva and L. Getoor. Privacy in social networks: A survey. In *Social Network Data Analytics*, pages 277–306. Springer US, 2011.
29. J. Zhou, Z. Liu, and B. Li. Influence of network structure on rumor propagation. *Physics Letters A*, 368(6):458–463, 2007.
30. H. Zhu, C. Huang, and H. Li. Information diffusion model based on privacy setting in online social networking services. *Comput. J.*, 58(4):536–548, 2015.