Peer-to-Peer Social Networks

Enrico Franchi
Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Parma, Italy

Agostino Poggi
Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Parma, Italy

Michele Tomaiuolo
Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Parma, Italy

INTRODUCTION

In the last ten years, the pervasive adoption of social networking sites has deeply changed the web. Social web sites have attracted users with very weak interest in technology, including people that before the social networking revolution were not even regular users of other popular Internet services and computers in general (Stroud, 2008). The phenomenon is so widespread that many people started using social networking systems to ask questions directly to people instead of querying search engines (Morris et al., 2010) and in place of regular email. Moreover, some of the largest social networking sites constitute a separate and closed network (Sabbag, 2011). After the huge success of the early social networking systems, many other players came in the social networking market and nowadays hundreds of different social networking systems exist. Even if the social networking systems are greatly dissimilar in their user base and functionality, they are almost always centralized systems. The centralized nature allows a simple browser-based user experience and, moreover, many algorithms, e.g., friend suggestion, are far easier and more efficient to implement in this setting. However, it also presents many drawbacks, e.g., lack of privacy, lack of anonymity, risks of censorship and operating costs**.** The goal of this article is to briefly introduce social networks, to show their relationships with peer-to-peer and multi-agent systems, and to discuss about the use of peer-to-peer and multi-agent systems in development of social network systems.

BACKGROUND

A social network is traditionally defined as a structure consisting of a finite set of actors and the relation or relations defined on them, where an actor is simply a discrete individual or a social unit (Wasserman & Faust, 1994). A social networking system is a web-site allowing users to have a profile and managing their online social network, i.e., it allows them to: (1) construct a profile which represents them in the system; (2) create a list of users with whom they share a connection and (3) navigate their list of connections and that of their friends (Ellison, 2007).

Although we agree that self-presentation and social network management are extremely important and necessary components of a social networking system, we believe that the social networking revolution is far more related to the paradigm shift that transformed most people from mere consumers of information to full-fledged information producers. Most people create information which is essentially personal and, then, it is mainly of interest for friends and acquaintances. Before the social web revolution such information used to be essentially lost in the web, while, nowadays social networking systems are able to deliver the information to the "right" people.

After the huge success of the early social networking systems, many other players came in the social networking market and nowadays hundreds of different social networking systems exist. Even if the social networking systems are greatly dissimilar in their user base and functionality, they are almost always centralized systems because of the access and implementation advantages.

DOI: 10.4018/978-1-4666-5888-2.ch663

A minor drawback is that scaling centralized systems to tens or hundreds of million of users is not an easy task. At any rate, we consider this drawback as a minor one, since the problem can be solved providing enough resources. However, the huge operative costs of supporting the infrastructure necessary to provide the service to millions of users can only be justified with robust business plans. While some social networking services have extremely differentiated business models (McGrath, 2010), for most of them the primary source of income is advertisement and consequently they have a strong motive for: (1) using user provided data to increase performance for that purpose and (2) even giving access to authorized commercial third parties to the raw data. This behavior poses serious threats to privacy and data protection issues, especially considering that there is no clear legislation on what uses of the user data are legittimate, and regarding the conditions for disclosing the data to third parties, especially when the subjects involved are from different countries.

Another problem is that social networking systems have terms of service that their users give to the system operators a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to the submitted content (Facebook, 2013; Twitter, 2013). Such terms are needed for legal reasons: in order to serve webpages containing the users' data (e.g., their profile page) the service provider needs some rights over that data; it is nonetheless true that users are essentially allowing the service providers to do with the data whatever they want for free. Moreover, most of the times, the users themselves have not easy and streamlined ways to obtain all the data they inserted in the system in a semantically meaningful or at least in a structured way; this (1) is a serious lock-in problem in its own right and (2) hinders users' trust in the platform. Most social networking platforms do not provide their users with easy and standard ways to export user submitted contents in a structured way. According to Fitzpatrick and Lueck (2010) this issue (1) is similar to a serious lock-in problem in its own right, and (2) it hinders users' trust in the platform.

The last problem with centralized social networking system is that service providers are in the position to effectively perform a-priori or a-posteriori censorship, or to disclose all the information they have, no matter how private, to other entities. They can perform such actions either motivated by selfish interests or forced under legal terms and other forms of pressure.

PEER-TO-PEER SYSTEMS AND SOCIAL NETWORKS

Peer-to-Peer (P2P) define an open and decentralized overlay network on top of the Internet that users can use for directly communicating to find and share resources, often music and movie files (Schollmeier, 2001). Such networks are one of the few largest distributed computing systems ever, and more surprisingly, they can run with great stability and resilient performance in face of possibly the most ferocious dynamics (Qiu & Srikant, 2004).

Thus, the use of P2P technologies for the development of social network is not only viable, but also highly desirable (Wang et al., 2006). First of all, P2P systems essentially achieve automatic resource scalability, in the sense that the availability of resources is proportional to the number of users. This property is especially desirable for media sharing social networking systems, considering the exceptionally high amount of resources needed. Secondly, the popularity over time of most content on such systems exhibits either a power-law or an exponential behavior and is consequently well suited for P2P distribution (Zink et al., 2009), possibly with fallback strategies for less popular content.

Regarding censorship issues, a P2P system essentially solves them by design. Without a central entity, nobody is in the position of censoring data systematically nor may be held legally responsible for the diffusion of censurable data: the sole owners and responsible of the data are the users themselves. Unfortunately, P2P systems, and especially Distributed Hash Table (DHT) based ones, may be still liable to attacks meant to disrupt the system functionality (Urdaneta et al., 2011), often based on the introduction of a large number of Sybil nodes and the diffusion of bogus information. However, the most popular DHT systems are significantly robust because of the high redundancy they achieve by using data replication and a redundant routing mechanism. Usually, the countermeasures are based on some notion of "trust," based on either certification authorities or some reputation mechanism (Aiello & Ruffo, 2012). Common consensus algorithms, including Byzantine agreement, have also been proposed and applied (Balfe et al., 2005; Anceaume et al., 2008).

Although peer-to-peer systems overcome the weakness of a single point of failure, there are some

Related Content