
Social computing: the state of the art

Justin Zhan* and Xing Fang

Department of Computer Science,
North Carolina A&T State University,
1601 East Market Street, Greensboro, NC, 27410, USA
E-mail: zzhan@ncat.edu
E-mail: xfang@ncat.edu
*Corresponding author

Abstract: Social computing can be broadly defined as computational facilitation of social studies and human social dynamics as well as design and use of information and communication technologies that consider social context. Novel social services and applications developed based on social computing have profoundly affected nowadays people's life. However, as an emerging research field, it gathers numerous researchers who tend to contribute cutting-edge research work on social computing. In this paper, we provide a brief overview towards the state of art of social computing.

Keywords: social computing; social networks; social media; social behaviour.

Reference to this paper should be made as follows: Zhan, J. and Fang, X. (2011) 'Social computing: the state of the art', *Int. J. Social Computing and Cyber-Physical Systems*, Vol. 1, No. 1, pp.1–12.

Biographical notes: Justin Zhan is the Director of iLab within the Department of Computer Science at North Carolina A&T State University. His research interests include social network science, social computing, information assurance, data mining and simulation tool development. He has served as a conference general chair, programme chair, publicity chair, workshop chair, and programme committee member for over 150 international conferences and as an editor-in-chief, editor, associate editor, guest editor, editorial advisory board member and editorial board member for 30 journals. In recent years, he has published 130 articles in peer-reviewed journals and conference proceedings.

Xing Fang is a graduate student at the Department of Computer Science, North Carolina A&T State University. His research interest includes social computing and information assurance. He has received his Master degree from Dakota State University and Bachelor degree from Northwestern Polytechnical University, China.

1 Introduction

Social computing can be broadly defined as computational facilitation of social studies and human social dynamics as well as design and use of information and communication technologies that consider social context. It is also a general term in

computer science that is concerned with the intersection of social behaviour and computational systems. Early work involving social computing exists in the area of social network analysis, which incorporates the usage of a set of theories, models, and applications for the analysis of social structures. With the evolution of computers and network technologies, social computing has been embedded new contents. A large number of novel applications as well as services facilitating collective action and online social interaction with rich exchange of multimedia information and evolution of aggregate knowledge are largely referred as social computing (Parameswaran and Whinston, 2007). Typical examples include online social networks, blogs, peer-to-peer networks, and other type of online communities. Since these applications or services usually offer relatively less technological requirements to their users, the ease of use makes such products grow rapidly. Ranging from business customers to personal users, social computing has been the backbone of today's information technology.

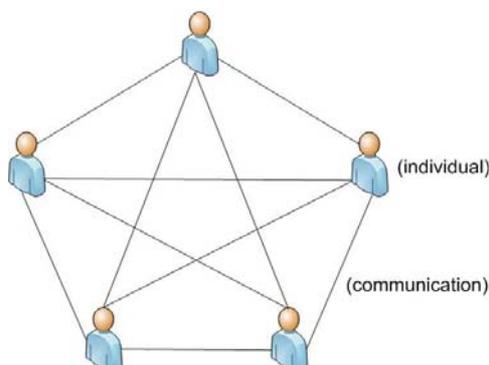
A new social era began with the prosperity of those applications which proves that social computing is becoming more indispensable for today's people's life. In this paper, we provide a brief overview towards social computing and introduce the papers published in the first issue. We first provide a brief overview towards some selected directions of social computing which includes social networks, social network analysis, social behaviour modelling, social signal processing (SSP), and information security and privacy on social networks. We then introduce some cutting-edge research work on the selected directions of social computing.

2 Overview of the selected directions of social computing

2.1 Social networks and social network analysis

A social network is a social structure which derives from the general human society according to certain scope or relationships. In one sense, it resembles as a graph consisting of nodes and edges. The nodes stand for entities such as individuals, groups, or organisations, while the edges are the whole collection of relationships existing in human society. Figure 1 is an example of a social network indicating an academic group.

The study of social network can be traced back to decades ago. In the early work, Tichy et al. (1979) introduced a social network approach in analysing organisations by examining the relationships of objects within them. Later, researchers found the recruitment of an organisation's social movements is effected by its social network attributes (Snow and Zurcher, 1980). Along with the study of social networks, Krackhardt (1987) provided cognitive social structures as the solution of network analysis problems. As a solid way to make progress, some review work is considered to be as equally important as the cutting edge research. Scott's (1988) paper reported both classical sociology and recent scientific work on social network analysis. Similarly, a book written by Wasserman and Faust (1994) was published six years later, the first book to provide a comprehensive overview of the methodology of and applications on social networks.

Figure 1 An example of a social network (see online version for colours)

After 2000, research has been focused on extracting useful knowledge using social network analysis. Freeman (2000) made important progress in social network visualisation. A model which has the capability to deal with network search problems was created based on searching recognisable personal identities through social networks (Watts et al., 2002). Sabater and Sierra (2002) presented a system using social network analysis to calculate reputations in multi-agent systems. Given the fact that a group of people has the ability to influence one another so as to trigger a cascade influence, a paper describing the strategy of choosing a few individuals in order to maximise the spread of influence through a social network was published (Kempe et al., 2003). A textbook of social network analysis was released in 2005 (Nooy et al., 2005). One year later, a social network evolution principle that is controlled by a combination of effects arising from the network topology and the organisational structure, where the network is embedded, was found by an empirical analysis of a social network (Kossinets and Watts, 2006).

The availability of Web 2.0 technology brought social network to the cyber world. Social networking sites (Boyd and Ellison, 2007) enable people to deploy their social activities through internet connections. This also triggers numerous research topics. Nowadays, social network is a popular while ambiguous concept. It can either represent a real human community; or can stand as a virtual network society fundamentally based on cyber network applications.

2.2 Human and social behaviour modelling and SSP

Human and social behaviour modelling (HSBM) provides mechanisms in reproducing human social behaviours and subsequent experimentation in various activities and environments (Liu et al., 2008). It has been an essential component of social computing. The interdisciplinary property of HSBM gathers researchers from different research fields, such as sociology, computer science, psychology, anthropology, and information systems, to share and study new methodologies.

The modelling of human cognitions requires the processing of imprecise human-centric concepts. Fuzzy systems modelling (FSM) (Pedrycz and Gomide, 2007) provides a venue that allows the formal reasoning and manipulation towards such concepts. The framework proposed by Yager (2008) adopted FSM as well as Dempster-Shafer theory (Shafer, 1976) to solve the problem of complex cognitive

concepts and unpredictability modelling for human behaviours. In addition to the modelling of human cognitions, human decision making and social interactions are crucial in terms of HSBM. For instance, in civil and environmental engineering, the design of safe egress is a key issue for crowd safety. The solution of such problem requires the modelling of crowd behaviours. In this case, Pan et al. (2006) presented a computational framework for incorporating human and social behaviours during emergency evacuations. They claimed that the proposed framework is able to model several human and social behaviours, such as competitive behaviour, queuing behaviour, herding behaviour, and bi-directional crowd flow.

With the popularity of the World Wide Web (WWW), its usage has been being involved in every aspect of people's home and work lives. As our dependence on the web increases, the amount of information that can be collected about an individual using the internet has the same trend. Hence, online users' behavioural information collecting has been paid much attention for years particularly by e-commerce and marketing firms in order to offer their customers better online shopping experiences. Sismeiro and Bucklin (2004) developed a predictive model of online purchase behaviour by using clickstream data collected from a car-selling website. They contended that the model has superior predictive performance especially during the task sequence. Montgomery et al. (2004) introduced a dynamic multinomial profit model for the analysis of path information of web browsing. It is believed that the model can also be used to personalise web designs and product offering. Robinson et al. (2008) introduced an online-users' behavioural analysis and modelling methodology based on their individual web browsing activities. Meanwhile, the method can be applied in security realm to enhance computer security via detecting malicious or anomalous online user behaviours.

Human face-to-face communication conveys both verbal information and non-verbal social signals such as vocal behaviour, facial expressions, and body postures and gestures which last for a relatively short time (Vinciarelli et al., 2009b). It is the common sense that current computers are socially ignorant. Thus, SSP is an emerging research domain that aims at provides computers the ability of recognising, and predicting (Pentland, 2008) social signals. However, the process for developing automated systems for SSP can be quite difficult (Vinciarelli et al., 2009a). The first challenge in SSP, according to Pentland (2008), is to automatically detect and measure the signals. Vinciarelli et al. (2009b) specified the problem into four sub-problems:

- 1 recording the scene
- 2 detecting people in it
- 3 extracting audio and/or visual behavioural cues displayed by people detected in the scene and interpreting this information in terms of social signals conveyed by the observed behavioural cues
- 4 sensing the context in which the scene is recorded and classifying detected social signals into the target social-behaviour-interpretative categories in a context-sensitive manner.

In addition, Vinciarelli et al. (2009a) also pointed out the future challenges of SSP:

- 1 tightening of the collaboration between social scientists and engineers
- 2 the need of implementing multi-cue, multimodal approaches to SSP

- 3 the use of real-world data
- 4 the identification of applications likely to benefit from SSP.

2.3 Information privacy and security on social networks

Social networks may maintain a very large amount of user data (personal information), which leads to one main issue that is privacy-related user data revelation (Blakely, 2007; Soghoian, 2009). Personal information, such as interests, contact information, photos, activities, associations and interactions, once revealed, may incur various magnitudes of impact, ranging from unexpected embarrassment or reputational damage (Rosenblum, 2007) to identity theft (Strater and Lipford, 2008). Despite the known negative consequences, effectively managing privacy for social network can be quite tricky. One reason is that different individuals have different levels of privacy-related expectations towards their information. For instance, some of them may be willing to publish their personal profiles tending to potentially develop more friendships, while others may worry about the exposure of their identities so as to only reveal the profiles to their close friends. In other situations, people are even willing to disclose their personal information to anonymous strangers rather than acquaintances (Gross and Acquisti, 2005). Unfortunately, people do not often care about their privacy either. Gross and Acquisti (2005) found that only a few students change the default privacy preferences on Facebook by analysing and evaluating the online behaviour as well as the amount of private information disclosed from 4,000 students in Carnegie Mellon University. On the other hand, Liu and Maes (2005) pointed out that “over a million self-descriptive personal profiles are available across different web-based social networks”. Thus, the lack of users’ privacy awareness and the ease of privacy exposure on social network attract researchers’ attentions. Krishnamurthy and Wills (2008) found that between 55% and 90% of users in popular social networks set their profile information publicly viewable and their activity is being tracked by the third party domains. Furthermore, Krishnamurthy and Wills (2010) examined the leakage of personal identifiable information, the information that may disclose personal identities by itself or through combing with other public information, on social networks. Zhou et al. (2008) concluded anonymisation techniques, which can be eventually applied to preserve privacy for social network data. Chen and Shi (2009) summarised the research of social network privacy by topics, including, privacy disclosure and attack technique, privacy-preserving collaborative social network, and business model of privacy protection.

Apart from privacy, social networks also associate with several security issues. For instance, with the ease of personal information access, social network makes itself a good place for social engineering (Nagy and Pecho, 2009). Furthermore, Luo et al. (2009) emphasised that spam, malicious programs, and phishing can be the most prevalent threats among social networks. To make matters worse, people are lacking of security concerns and basic security knowledge towards social networks. Meanwhile, social network is attracting researchers to develop security countermeasures. Decentralised or distributed systems are vulnerable to sybil attack (Douceur, 2002), where a small number of entities pretending to be multiple ones so as to compromise a large fraction of the systems. Correspondingly, SybilGuard, a protocol designed to against sybil attack via social networks, was presented by Yu et al. (2006). Based upon the observation that social network has the capability to limit attack edges, which are the ones connecting

honest nodes and sybil (malicious) nodes in social network, by leveraging trust relationships built within real social network, SybilGuard is able to effectively against sybil attack by bounding both the number and the size of Sybil node groups. Later, Yu et al. (2008) introduced SybilLimit, a similar sybil attack prevention protocol as SybilGuard. SybilLimit enhances the protocol performance by reducing a factor of $\theta(\sqrt{n})$ from SybilGuard. A similar approach inspired by SybilGuard was proposed by Hota et al. (2007) to against sybil attack. Instead of random walk in SybilGuard, their approach adopts single source and multiple destinations routing protocol to control the number and the size of sybil groups.

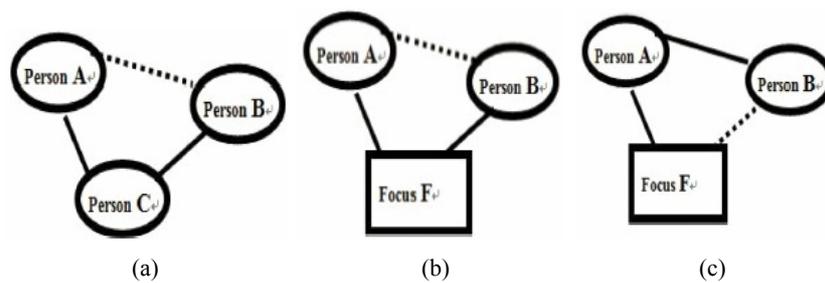
3 Social computing: the state of the art

3.1 Social networks and social network analysis

The formation of a certain social network is often based on some certain events. This so-called evolving social network has its sets of nodes and edges changed over time because of the joining of new nodes as well as the leaving of old ones. According to Qiu et al. (2011), it is the natural way that the growth dynamics of such a social network can be captured by an event-driven model, in which an event has participants (nodes), whose relationships are referred to the connections (edges). The event-driven model consists of an event-driven framework and a hybrid growth model. The framework deals with the social network including events adding. The hybrid growth model is designed to incorporate the attachedness and locality of the social network, since both of the factors affect the form of the new edges.

Douban, a popular Chinese online social network, serves users in media recommendations. As its user, one can share her media interests under the profile information. Users are also able to make online friends and join discussion groups on different topics. As of the formation of friendships, McPherson et al. (2001) identified three basic patterns of homophily (Figure 2).

Figure 2 Homophily in a social network



Those three patterns are: triadic closure [Figure 2(a)], focal closure [Figure 2(b)], and membership closure [Figure 2(c)]. Triadic closure creates new friendship between person A and B via their mutual friends C; focal closure builds up the same friendship just like triadic closure does except that the mutual friend is switched to a common focus; membership closure eventually allows person B to become a participant of a focus due to person B's friendship with A. Based upon the monitor towards 10,000 Douban users?

profiles, Yu and King (2010) addressed that the triadic closure is a major force for the formation of online friendships, whereas certain types of focal closure even have larger effect than triadic closure.

Cultural items affect the adoption of similar ideas, behaviours, opinions, and topics. The study of cultural items and social meditation is crucial to social scientists who want to know which kind of individuals are more or less likely to pass on some pieces of information and which network positions can help the diffusion of some items. Menezes et al. (2011) presented a method for the detection of bursts of activity at the semantic level, and described a probabilistic model to quantify temporal relationships between blogs. The process of activity detection consists of linguistic tagging, term filtering, and term merging. The result of activity detection process is a set of topics and each topic's temporal relationships with certain blogs. The probabilistic model, in turn, can quantify temporal relationships between blogs by computing a dyadic precursor score from one blog to the other.

Contending that social relations are difficult to be measured especially just via single dataset, Karikoski and Nelimarkka (2011) examined the used of different datasets to measure social relations, which are defined as physical presence, online communication and presence, or direct communication. In their work, they adopted one mobile phone dataset and one online social media service dataset. The mobile phone dataset contains data like phone call history and SMS messages. The online social media service dataset has the knowledge of social structures based upon friendships and so on. Based on their work, they claimed that the study of social relations should be conducted under multiple datasets.

A social network may consist of several communities that are either disjointed or overlapped. Traditional methods to identify community structure are only suitable to those disjointed communities, while recent proposed methods, although have taken overlapped communities into account, failed to examine the characteristics of such communities. Kelley et al. (2011) first suggested that a community should meet two minimum requirements that are connectedness and local optimality. Based on the study of previous overlapping communities detecting methods, they then presented empirical evidence of the existence of a large amount of significant overlap in network of blogs that proves the deficiency of the traditional approach for identifying community structure.

With rapid growth of online social networks, it can be very expensive to measure their properties, of which require the knowledge of the entire networks. In this case, acquiring the size information for a certain social network becomes critical, such as the number of users that belong to the online social network. To tackle the problem, Ye and Wu, whose paper is included in this issue, introduced three online social network size estimators, maximum likelihood estimator (MLE), mark and recapture (MR), and random walkers (RW). Both MLE and MR require uniformly sampling a certain amount of users from the network, whereas RW requires friend lists of users to be available in order to conduct the random walk. For the MLE, they developed an algorithm that 70 times faster than the naïve linear probing method; for the MR, a better estimation of the network size is applied to Twitter's public timeline service; they also extended the RW to estimate other network properties like clustering coefficient.

The similarity between two social networks is important in terms of understanding both networks' graphical form. To achieve the similarity comparison, Macindoe and Richards (2011) proposed a comparison technique of using the networks' sub-graph. In their approach, a network can be abstractly represented via three sub-graphical features.

They are leadership, bonding, and diversity. Leadership (L) is a measure of the extent to which the edge connectivity of a graph is dominated by a single vertex. Bonding (B) measures the graph's triadic closure. Diversity (D) is a measure based on the number of edges in a graph, of which end vertices are disjoint. Hence, the similarity is represented by the earth mover's distance (Pele and Werman, 2009) between the LBD's distributions of the networks.

In social tagging systems, tag clouds are widely believed to be developed to improve user experience on content navigation. In practice, tag clouds aggregate and display tags, and corresponding resources, from various sources. Helic et al. (2011) proposed to validate the navigability assumption of tag clouds. Based on the analysis of three tagging datasets, they found that the navigability of tag clouds is not always effective. In some circumstance, the interface design of tag clouds may impair their navigability.

3.2 Social behaviour modelling

Blogosphere has huge popularity that gathers a very large amount of online users. However, current methodology to identify special users of a certain blog is to generate a list of active and popular users. Moon and Han (2011) found that a list of such users may not necessarily be influential. Moon and Han (2011) defined that influencers are the ones "who have influential power to the point that they can change others' thinking or behaviours". Therefore, they proposed the quantifying influence model (QIM) that measures influence score for bloggers. The QIM has two components, interpersonal similarity and degree of information propagation. Interpersonal similarity measures homophious ties between active readers and actual bloggers, while degree of information propagation is the degree of information spreading via weighted bridging readers. The final influential score is a sum of both weighted interpersonal similarity and degree of information propagation.

3.3 Social signal processing

Human interaction geometry largely refers to human social interactions that convey non-verbal social signals, such as turning towards each other. Groh and Lehmann (2011) presented an interaction model, with respect to interaction geometry, to study interaction geometry in the view of the detection of social situations. By employing mobile devices, they measured geometrical interaction data using the proposed model.

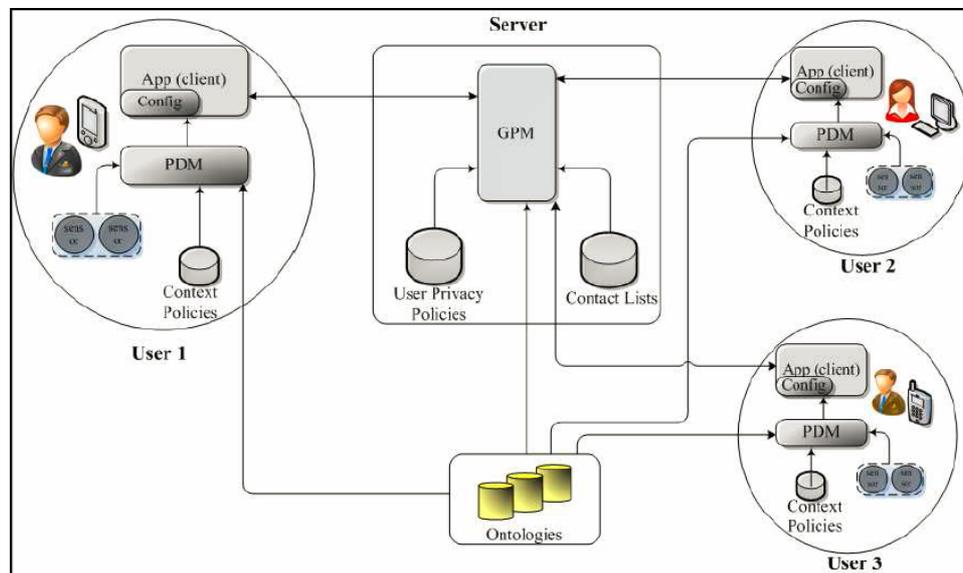
3.5 Social network privacy and security

Traditional database anonymity techniques, like k-anonymity (Sweeney, 2002), p-sensitivity (Truta and Vinay, 2006), l-diversity or t-closeness (Machanavajjhala et al., 2007) treats data either as public or as private. When it comes to social networks, it requires data to be assumed as public then treated as private. This generates the problem that the traditional data anonymity techniques are not appropriate for social network data anonymisation. In other words, those techniques make the published social network data non-interactive. Thus, Beach et al. (2011) introduced a social network data anonymity model, namely q-Anon. The proposed model measures the ambiguity of published data in

the perspective of re-identification attack. The larger the value of q is, the higher the data's privacy.

A privacy sensitive architecture for context obfuscation (PCO) was developed by Rahman et al. (2011). PCO is used to protect privacy in pervasive online social networking applications, such as online community-based applications. The entire architecture (Figure 3) includes user component and server component. The profile data manager (PDM) of the user component manages contextual data provided by user or acquired from device sensors. The granularity-based privacy module from the server component is designed to protect the privacy of received contextual data by enforcing user-defined privacy policies based on contact lists.

Figure 3 The architecture of PCO (see online version for colours)



Source: Rahman et al. (2011)

4 Conclusions

Social computing plays more and more important role in today's cyber-related applications that have profoundly affected people's daily life. A large number of social computing applications, such as online social networks, blogs, peer-to-peer networks, micro-blogs, social tagging systems, photo and video sharing websites, and other types of online social communities, have gained much popularity. Furthermore, as an emerging research field, social computing gathers numerous researchers who tend to contribute cutting-edge research work on social computing. In this paper, we provide a brief overview towards social computing that includes most recent research work on it.

References

- Beach, A., Gartrell, M. and Han, R. (2011) 'q-Anon: practical anonymity for social networks', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Blakely, R. (2007) *Does Facebook's Privacy Policy Stack Up?*, available at http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2430927.ece (accessed on 9 September 2011).
- Boyd, D. and Ellison, N. (2007) 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, Article 11.
- Chen, X. and Shi, S. (2009) 'A literature review of privacy research on social network sites', *Proceedings of International Conference on Multimedia Information Networking and Security*, Hubei, China, pp.93–97.
- Douceur, J. (2002) 'The sybil attack', *The 1st International Workshop on Peer-to-Peer Systems*, London, UK, pp.251–260.
- Freeman, L. (2000) 'Visualizing social networks', *Journal of Social Structure*, Vol. 1, No. 1.
- Groh, G. and Lehmann, A. (2011) 'Deducing evidence for social situations from dynamic geometric interaction data', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Gross, R. and Acquisti, A. (2005) 'Information revelation and privacy in online social networks', *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*, Alexandria, Virginia, USA, pp.71–80.
- Helic, D., Trattner, C., Strohmaier, M. and Andrews, K. (2011) 'Are tag clouds useful for navigation? A network-theoretic analysis', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Hota, C., Lindqvist, J., Karvonen, K., Jaaski, A. and Mohan, J. (2007) 'Safeguarding against sybil attacks via social networks and multipath routing', *The International Conference on Networking, Architecture, and Storage*, Guilin, China, pp.122–132.
- Karikoski, J. and Nelimarkka, M. (2011) 'Measuring social relations with multiple datasets', *International Journal of Social Computing and Cyber-Physical System*, August.
- Kelley, S., Goldberg, M., Mertsalov, K., Magdon-Ismail, M. and Wallace, W. (2011) 'Overlapping communities in social networks', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Kempe, D., Kleinberg, J. and Tardos, E. (2003) 'Maximizing the spread of influence through a social network', *International Conference on Knowledge Discovery and Data Mining*, Washington, DC, USA.
- Kossinets, G. and Watts, D. (2006) 'Empirical analysis of an evolving social network', *Science*, Vol. 311, No. 5757, pp.88–90.
- Krackhardt, D. (1987) 'Cognitive social structures', *Social Networks*, Vol. 9, No. 1, pp.109–134.
- Krishnamurthy, B. and Wills, C. (2008) 'Characterizing privacy in online social networks', *Proceedings of the 1st Workshop on Online Social Networks*, Seattle, WA, USA, pp.37–42.
- Krishnamurthy, B. and Wills, C. (2010) 'On the leakage of personally identifiable information via online social networks', *ACM SIGCOMM Computer Communication Review*, Vol. 40, No. 1, pp.112–117.
- Liu, H. and Maes, P. (2005) 'Interestmap: harvesting social network profiles for recommendations', *Proceedings of the Beyond Personalization 2005 Workshop*, San Diego, CA, USA, pp.54–59.
- Liu, H., Salerno, J. and Young, M. (Eds.) (2008) *Social Computing, Behavioral Modeling, and Prediction*, Springer, New York, USA.
- Luo, W., Liu, J., Liu, J. and Fan, C. (2009) 'An analysis of security in social networks', *The 8th International Conference on Dependable, Autonomic and Secure Computing*, Chengdu, China, pp.648–651.

- Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkatasubramanian, M. (2007) 'l-diversity: privacy beyond k-anonymity', *ACM Transactions on Knowledge Discovery from Data*, Vol. 1, No. 1.
- Macindoe, O. and Richards, W. (2011) 'Comparing networks using their fine structure', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- McPherson, M., Smith-Lovin, L. and Cook, J. (2001) 'Birds of a feather: homophily in social networks', *Annual Review of Sociology*, Vol. 27, No. 1, pp.415–444.
- Menezes, T., Roth, C. and Cointet, J. (2011) 'Finding the semantic-level precursors on a blog network', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Montgomery, A., Li, S., Srinivasan, K. and Liechty, J. (2004) 'Modeling online browsing and path analysis using clickstream data', *Marketing Science*, Vol. 23, No. 4, pp.579–595.
- Moon, E. and Han, S. (2011) 'A qualitative method to find influencers using similarity-based approach in the blogosphere', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Nagy, J. and Pecho, P. (2009) 'Social networks security', *The 3rd International Conference on Emerging Security Information, Systems, and Technologies*, Athens, Greece, pp.321–325.
- Nooy, W., Mrvar, A. and Batagelj, V. (2005) 'Exploratory social network analysis with Pajek', *Structural Analysis in the Social Sciences*, Vol. 27, Cambridge University Press, UK.
- Pan, X., Dauber, K., Han, C. and Law, K. (2006) 'Human and social behavior in computational modeling and analysis of egress', *Automation in Construction*, Vol. 15, No. 4, pp.448–461.
- Parameswaran, M. and Whinston, A. (2007) 'Social computing: an overview', *Communications of the Association for Information Systems*, Vol. 19, No. 1, pp.762–780.
- Pedrycz, W. and Gomide, F. (2007) *Fuzzy Systems Engineering: Towards Human-centric Computing*, John Wiley & Sons, New York.
- Pele, O. and Werman, R. (2009) 'Fast and robust earth mover's distances', *Proceedings of the International Conference on Computer Vision*.
- Pentland, A. (2008) *Honest Signals: How they Shape our World*, The MIT Press, Cambridge, Massachusetts, USA.
- Qiu, B., Ivanova, K., Yen, J., Liu, P. and Ritter, F. (2011) 'Event-driven modelling of evolving social networks', *International Journal of Social Computing and Cyber-Physical Systems*.
- Rahman, F., Hoque, M., Kawsar, F. and Ahamed, S. (2011) 'User privacy protection in pervasive social networking applications using PCO', *International Journal of Social Computing and Cyber-Physical Systems*, August.
- Robinson, D., Berk, V. and Cybenko, V. (2008) 'Online behavioral analysis and modeling methodology', *Social Computing, Behavioral Modeling, and Prediction*, Springer, New York.
- Rosenblum, D. (2007) 'What anyone can know: the privacy risks of social networking sites', *IEEE Security and Privacy*, Vol. 5, No. 3, pp.40–49.
- Sabater, J. and Sierra, C. (2002) 'Reputation and social network analysis in multi-agent systems', *International Conference on Autonomous Agents and Multiagent Systems*, Bologna, Italy.
- Scott, J. (1988) 'Social network analysis', *Sociology*, Vol. 22, No. 1, pp.109–127.
- Shafer, G. (1976) *A Mathematical Theory of Evidence*, Princeton University Press, USA.
- Sismeiro, C. and Bucklin, R. (2004) 'Modeling purchase behavior at an e-commerce web site: a task-completion approach', *Journal of Marketing Research*, Vol. 41, No. 3, pp.306–323.
- Snow, D. and Zurcher, L. (1980) 'Social networks and social movements: a microstructural approach to differential recruitment', *American Sociological Review*, Vol. 45, No. 5, pp.787–801.
- Soghoian, C. (2009) *The Next Facebook Privacy Scandal*, available at http://news.cnet.com/8301-13739_3-9854409-46.html.

- Strater, K. and Lipford, H. (2008) 'Strategies and struggles with privacy in an online social networking community', *Proceedings of the 22nd British HCI Group Annual Conference*, Liverpool, UK, pp.111–119.
- Sweeney, L. (2002) 'k-anonymity: a model for protecting privacy', *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, No. 5, pp.557–570.
- Tichy, N., Tushman, M. and Fombrun, C. (1979) 'Social network analysis for organizations', *The Academy of Management Review*, Vol. 4, No. 4, pp.507–519.
- Truta, T. and Vinay, B. (2006) 'Privacy protection: p-sensitive k-anonymity property', *Proceedings of the 22nd International Conference on Data Engineering Workshops*.
- Vinciarelli, A., Pantic, M. and Boulard, H. (2009a) 'Social signal processing: survey of an emerging domain', *Image and Vision Computing*, Vol. 27, No. 12, pp.1743–1759.
- Vinciarelli, A., Salamin, H. and Pantic, M. (2009b) 'Social signal processing: understanding social interactions through nonverbal behavior analysis', *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp.42–49.
- Wasserman, S. and Faust, K. (1994) *Social Network Analysis: Methods and Applications*, Cambridge University Press, UK.
- Watts, D., Dodds, P. and Newman, M. (2002) 'Identity and search in social networks', *Science*, Vol. 296, No. 5571, pp.1302–1305.
- Yager, R. (2008) 'Human behavioral modeling using fuzzy and Dempster-Shafer theory', *Social Computing, Behavioral Modeling, and Prediction*, pp.89–99, Springer, New York, USA.
- Yu, H., Gibbons, P., Kaminsky, M. and Xiao, F. (2008) 'SybilLimit: a near-optimal social network defense against sybil attacks', *The IEEE Symposium on Security and Privacy*, Oakland, California, USA, pp.3–17.
- Yu, H., Kaminsky, M., Gibbons, P. and Flaxman, A. (2006) 'SybilGuard: defending against sybil attacks via social networks', *The Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Pisa, Italy, pp.267–278.
- Yu, L. and King, V. (2010) 'The evolution of friendships in Chinese online social networks', *IEEE International Conference on Social Computing*, 20–22 August, Minneapolis, pp.81–87.
- Zhou, B., Pei, J. and Luk, W. (2008) 'A brief survey on anonymization techniques for privacy preserving publishing of social network data', *ACM SIGKDD Explorations Newsletter*, Vol. 10, No. 2, pp.12–22.