

# B

## Behavior Modeling in Social Networks

Meng Jiang  
Department of Computer Science and  
Engineering, University of Notre Dame, Notre  
Dame, IN, USA

### Synonyms

[Applied behavior analysis in social networks](#);  
[Behavioral analytics in social networks](#)

### Glossary

CF	Collaborative filtering
LDA	Latent Dirichlet Allocation: an effective topic model
OSNs	Online social networks
Power law	A functional relationship between two quantities where a relative change in one quantity results in a proportional relative change in the other quantity: one quantity varies as a power of another
RSs	Recommender systems
SBD	Suspicious behavior detection: detecting fake reviews, fake social accounts, spammers, fake relationships, and fraudsters

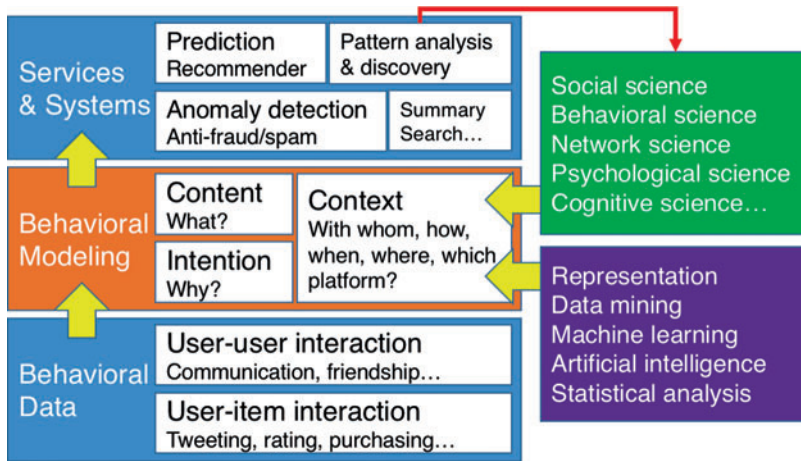
Social context	Contextual factors that determine users' behaviors in social environments such as influence, trust, and preference
UGC	User-generated content

### Definition

*Behavior modeling in social networks* is a core framework of the “data-to-knowledge-to-service” pipeline with behavioral data as input to support services and systems of the OSNs including precise recommendation and spam and fraud detection (Fig. 1). The main object in the behavioral setting is the behavior, which is the set of all signals generated by the users on the OSNs. The pipeline consists of the modules of collecting, understanding, and intervening behaviors. The behavior modeling focuses on understanding the major factors of the human behaviors such as behavioral content, context, and intention. Effective and efficient behavior modeling requires interdisciplinary knowledge: (1) scientific discovery in social science, behavioral science, and even psychology uncovers the underlying factors of human behaviors; (2) advanced methods and techniques in the area of computer science provide solid learning models for the core framework.

### Introduction

The development of social media has enabled the collection of behavioral data of unprecedented



**Behavior Modeling in Social Networks, Fig. 1** Behavior modeling is a core framework of the “data-to-knowledge-to-service” pipeline. The framework utilizes scientific discovery from social, behavioral, psychological, and cognitive sciences to uncover the underlying factors of user-user and user-item interactions. The major factors of human behaviors in social networks are

content, context, and intention. Then it models the factors for specific tasks such as prediction, summarization, and anomaly detection with modern data mining and machine learning methods. The real-world experimental practice develops the deep understanding of human behaviors as feedbacks in the pipeline

size and complexity. All social platforms have realized that great scientific and marketing values are contained in the millions of billions of behavioral records. Accurate prediction and detection of user behavior are key techniques for many social media applications, such as recommender systems (RSs), personalized search, and social marketing. *Behavior modeling* is significant in real applications and systems.

First, behavior modeling in social networks has countless marketing value in web service and information system. Social recommendation systems and social media marketing have become very important profit-making models. Social media closely connect users and provide them with a wide range of patterns and channels to acquire information and knowledge and even meet their shopping needs. Applications based on large-scale behavioral data, such as precise prediction on click and purchase behaviors and antifraud detection, have brought massive market values and economic returns.

Second, behavior modeling in social networks has great significance in the national product and security. Social media enable people to create, publish, and broadcast information with extreme

ease and speed. It altered the traditional environment of news and information dissemination which has been monopolized by the state and related institutions for centuries. Moreover, quicker and easier sharing and cooperation in social media are free from the huge cost of traditional business models. It amplifies the influence of individuals on productivity, state security, and social development.

In the field of computer science, behavior modeling is one of the most important scientific research problems.

First, user behaviors in social networks are richer and more complex than those in traditional life. Behaviors in social networks are mainly user-user interactions such as friendships, following relationships, interaction frequencies, and roles in the networks. User behaviors in social media are user-information interactions that contain rich contents including text, image, video, URL, and emoticon and many environmental aspects including device and geo-location. Behavioral data in complex social media environments is much richer than the data in traditional social networks: the number of users is at million or billion level, while the number of user behaviors

which can be represented as user-information interactions increases by millions of billions every day.

Second, behavior modeling in social networks needs supports from interdisciplinary research. Different social media services based on web technology create different behavioral mechanisms. However, behavioral analysis under these mechanisms cannot be solely conducted by the web technology. Knowledge from multiple research areas such as anthropology, anthropology, psychology, sociology, and communication studies has great significance in understanding user behaviors and uncovering rules of social environments. The ideas of behavioral models often come from hypothesis on user behavioral mechanisms that have been uncovered in these areas: researchers should answer the following questions. Why do users forward, share, or reject a received message in social media? Are their behaviors consistent and complementary in different social media platforms? Do users who have monetary incentives or fraudulent intentions generate suspicious behaviors? What are the differences between their suspicious behavioral patterns and normal users' patterns? Only by integrating interdisciplinary knowledge can we effectively analyze and model user behaviors in social media.

## Key Points

Behavior modeling has to face a few serious challenges brought by the large-scale behavioral data. The major challenges are as follows.

**High sparseness** Traditional behavior prediction methods including collaborative filtering techniques suffer from the problem of high sparseness of behavioral data. For example, the Netflix rating data are often sparse, bringing big errors in estimating correlations between users and movies and making rating predictions inaccurate.

**Heterogeneity** User behaviors that can be represented as user-item links create heterogeneous graphs in multiple aspects due to the complex environments of social media. First, behavioral link properties are different in different

social networks. In general, user behaviors form different types of graphs such as undirected graphs, directed graphs, bipartite graphs, weighted graphs, or hyper-graphs, which have been represented as symmetric matrix, asymmetric matrix, binary matrix, nonnegative matrix, or nonnegative tensor. Second, social networks include not only user nodes but also different types of nodes that represent information, contents, devices, and many other elements in the networks.

**Large volume and dynamics** The dynamics of user behaviors continuously input behavioral data into computational models of real systems. The systems are often broken down due to repetitive tasks of processing behavioral dynamics. For example, when there is a new user or a new message in Twitter, the computational complexity of updating and training behavioral data of billions of users is too high to practice. It is important to study incremental processing methods and online learning methods in large-scale social media.

**Complex intentions** Social media have become an important tool to broadcast information in this era: governments have realized the information cascades of high speed, wide range, and strong influence. Users look for useful information in social media, and at the same time, they spot suspicious behavioral phenomena of information manipulation. Social media services are seeking effective suspicious behavior detection (SBD) techniques. The common suspicious behaviors include lockstep following relationships by zombie followers and malicious web posts by fraudsters and spammers. For example, you can purchase 4000 Twitter followers with a cup of coffee.

## Historical Background

In the late 1970s, the behavioral approach to systems theory and control theory was initiated where the behaviors are signals compatible with the system. Since the twenty-first century comes, OSNs such as Facebook, Twitter, and LinkedIn emerge and attract billions of accounts; thus, the

signals from the users behind the systems are stored in the databases at a large scale. The behavior modeling in social networks is to understand the underlying patterns of human behaviors to facilitate the systems and services from the large collections of data.

Scientists have early realized that user preference that describes what content a user likes is an important driving factor for user behaviors. *Content-based analysis* used word distributions to represent users and items in news RSSs (Balabanović and Shoham 1997); however, it did not take use of the semantics inside the sparse word distributions. In 2003, latent Dirichlet allocation (LDA) was proposed to automatically group documents into topics according to dependencies between words and documents (Blei et al. 2003). Based on the advanced LDA, scholars proposed a series of preference-based methods (Liu et al. 2012). The personalized preference analysis discovered the topic-level social dynamics in Twitter text data (Narang et al. 2013).

Context awareness was first introduced by Schilit in 1994 to refer to the idea that computers react based on their environments (Schilit et al. 1994). In social networks, the users react or behave based on the environments including the time, geographical location, the social platform they are using, the channel they access the network, and their friends' words (Yuan et al. 2013; Liu and Aberer 2013). On one hand, the researchers dig into the details of the contextual information. Local and global contexts were exploited for social recommendation (Tang et al. 2013). On the other hand, they propose complicated, effective, and efficient models to represent the multifaceted behaviors, discover the behavioral patterns, and predict the missing behaviors (Jiang et al. 2014a).

The world of the Internet does not always tell truth. There are four categories of suspicious behaviors: traditional spam (web, email, and short message), fake review, social spam, and social link farming (Jiang et al. 2016b). Before the social networks appear, researchers have proposed several web spam and fake review spam detection techniques (Chirita et al. 2005; Xu et al. 2012). But the social networks are more complicated. In order to catch the suspicious behaviors in

Facebook or Twitter, we have to understand the behavioral intentions of the suspicious accounts. Therefore, in the last decade, the researchers focus more on detecting social spammers, fake followers, and fake Page Likes.

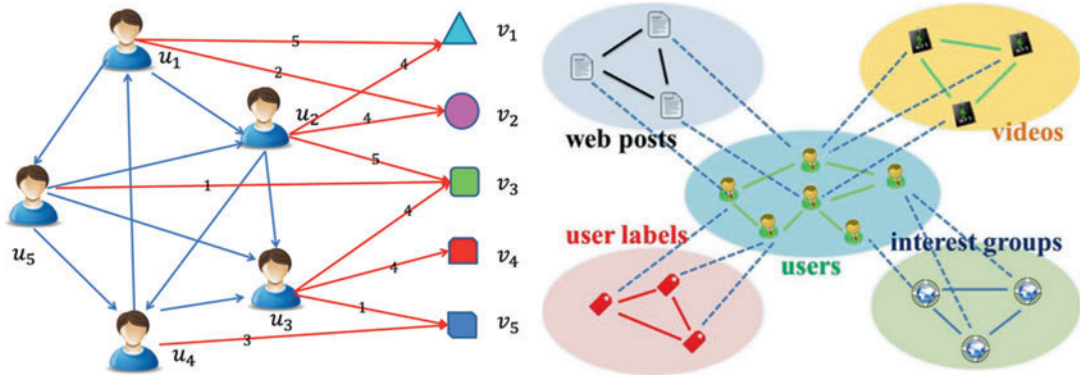
## Modeling Complex Behaviors in Social Networks

### Modeling Behavior Content

Users generate countless texts, images, and videos in social networks. However, the content data are often unstructured especially for the text (e.g., tweets, blogs, reviews, articles). Modeling behavior content refers to represent a user's interests so that the algorithms can match the items or the other users according to the user preference. The link prediction problem was introduced to the user-oriented applications (Liben-Nowell and Kleinberg 2007). Item nodes are used to represent the content information such as tweets, books, and movies. During the next years, researchers have taken many types of the items such as social tags, photos, videos, and interest groups (Jiang et al. 2012a). As shown in Fig. 2, matrix factorization techniques that represent the networks into matrices show high accuracy in predicting the missing values (Koren 2008; Koren et al. 2009), and random walk with restart methods can bridge different item domains to transfer the auxiliary knowledge over the networks (Jiang et al. 2015a). Modeling the behavior content into deep representations of the attributes and aspects of the items and events is a challenging problem.

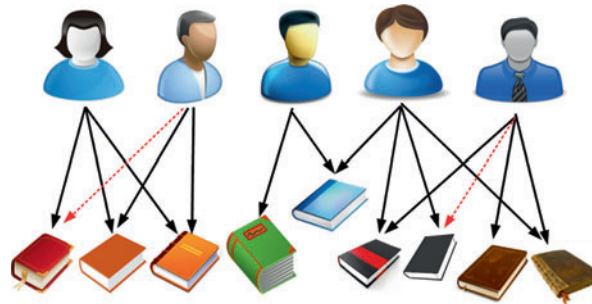
### Modeling Social Context

Social and behavioral sciences have fundamentally benefited the behavior modeling in a social contextual environment. One of the great breakthroughs is the *collaborative filtering* (CF) technique. CF is a method of making automatic predictions (filtering) about the interests of a user by collecting preferences or taste information from many users (collaborating). The underlying assumption of the CF approach is that if a person A has the same opinion as a person B on an issue, A is more likely to have B's opinion on a different issue  $x$  than to



**Behavior Modeling in Social Networks, Fig. 2** The content information including tweets, social tags, videos, and groups are represented as item nodes as well as user nodes. Matrix factorization and random walk techniques

perform well in predicting missing links on the networks. Though researchers have brought in many types of the items, such representations lose much knowledge of the items' attributes and aspects



**Behavior Modeling in Social Networks, Fig. 3** The underlying assumption of the CF approach is that if a person A has the same opinion as a person B on an issue, A is more likely to have B's opinion on a different issue x

than to have the opinion on x of a person chosen randomly. The left two persons have similar tastes and the right-hand two have similar tastes. So a CF approach assumes they will share more books in the future

have the opinion on x of a person chosen randomly (Sarwar et al. 2001; Liu et al. 2009; Koren 2010). For example, a CF recommendation system for television tastes could make predictions about which book shows a user should like given a partial list of that user's tastes, as shown in Fig. 3.

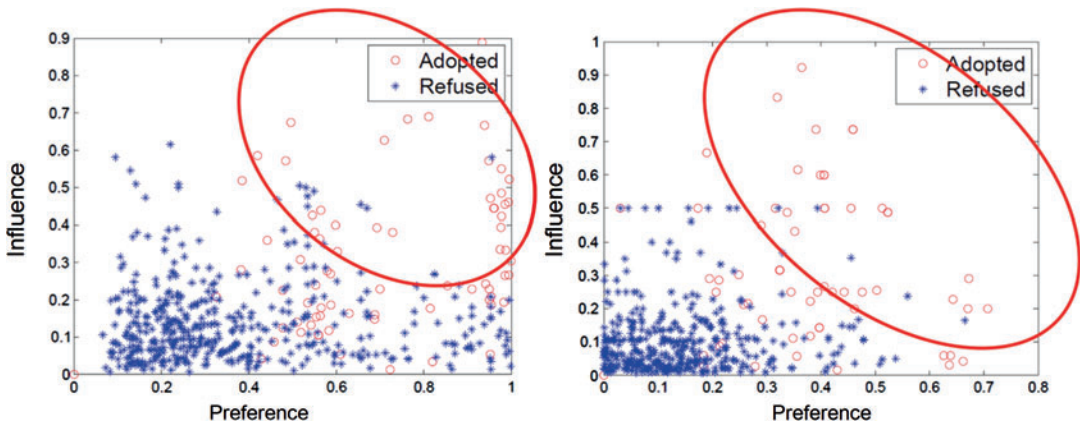
which is based on a probabilistic matrix factorization method to incorporate the two factors to improve the accuracy of social recommendation (Jiang et al. 2014b).

Psychological and sociological studies have provided individual preference and interpersonal influence affect user behaviors. Individuals are to some extent influenced by others, rather than making decisions independently (Bond and Smith 1996). As shown in Fig. 4, users intend to adopt items with higher preference scores and from higher influential friends in Facebook (left) or Twitter (right) networks (Jiang et al. 2012b). Researchers proposed a social contextual recommendation framework

**Modeling Cross Platform Context**

People often use multiple platforms to fulfill their different information needs. With the ultimate goal of serving people intelligently, a fundamental way is to get comprehensive understanding about user needs. How to organically integrate and bridge cross platform information in a human-centric way is important. A paucity of research works investigated cross domain behaviors based on transfer learning. They assumed either a fully overlapped shape (Zhong et al. 2014) or a non-

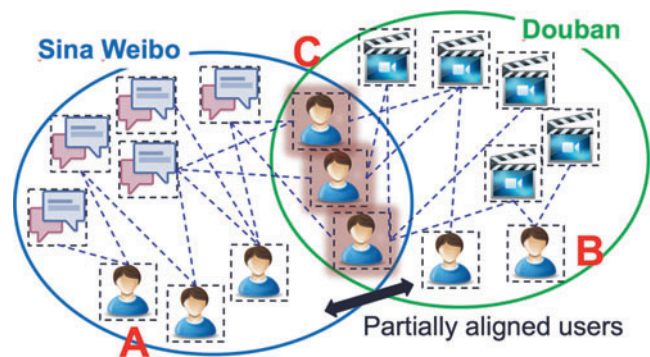




**Behavior Modeling in Social Networks, Fig. 4** Users intend to adopt items with higher preference scores and from higher influential friends in Facebook (*left*) or Twitter (*right*) networks

### Behavior Modeling in Social Networks,

**Fig. 5** The essential problem in cross platform behavioral prediction is how to fully exploit the small number of overlapped crowds to optimally bridge a user's behaviors in different platforms

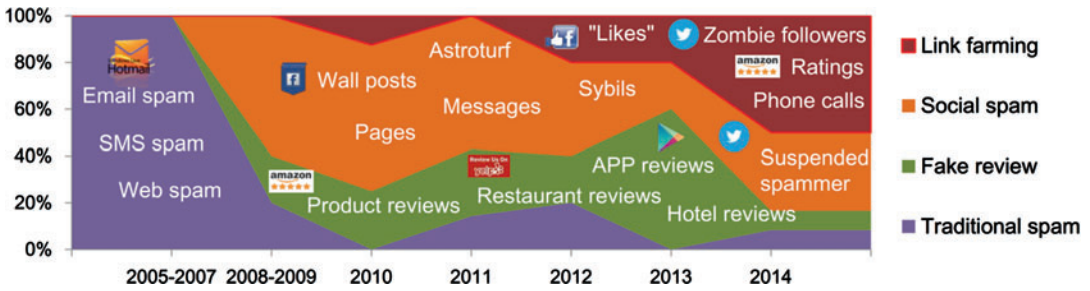


overlapped shape (Li et al. 2009) among the users across different platforms or domains. However, the real case is in the middle, where there are some common users (partially overlapped users) across the different platforms. The number of overlapped users is often small, and the number of explicitly known overlapped users is even less, due to the lacking of unified ID for a user across different platforms. Thus the essential problem in cross platform behavioral prediction is how to fully exploit the small number of overlapped crowds to optimally bridge a user's behaviors in different platforms (see Fig. 5). A novel semi-supervised transfer learning method XPTrans jointly optimizes users' latent features on different platforms to alleviate the sparseness (Jiang et al. 2016a). The latent space for user representation in one platform should be different from another. For different platforms, XPTrans allows different settings

for the latent dimensions. Data analysis shows that similarities between the overlapped users are consistent across platforms. XPTrans uses constraints of pairwise similarity to bring better flexibility. However, integrating multiple social network platforms for a better understanding of human behaviors still has a long way to go.

### Modeling Behavior Intention

As web applications such as Hotmail, Facebook, Twitter, and Amazon have become important means of satisfying working, social, information-seeking, and shopping tasks, suspicious users (such as spammers, fraudsters, and other types of attackers) are increasingly attempting to engage in dishonest activity, such as scamming money out of Internet users and faking popularity in political campaigns. Fortunately, commercially available suspicious behavior detection techniques can eliminate a



**Behavior Modeling in Social Networks, Fig. 6** The percentages of research works that focus on the four categories show tremendous progress in social spam detection and social link farming detection systems

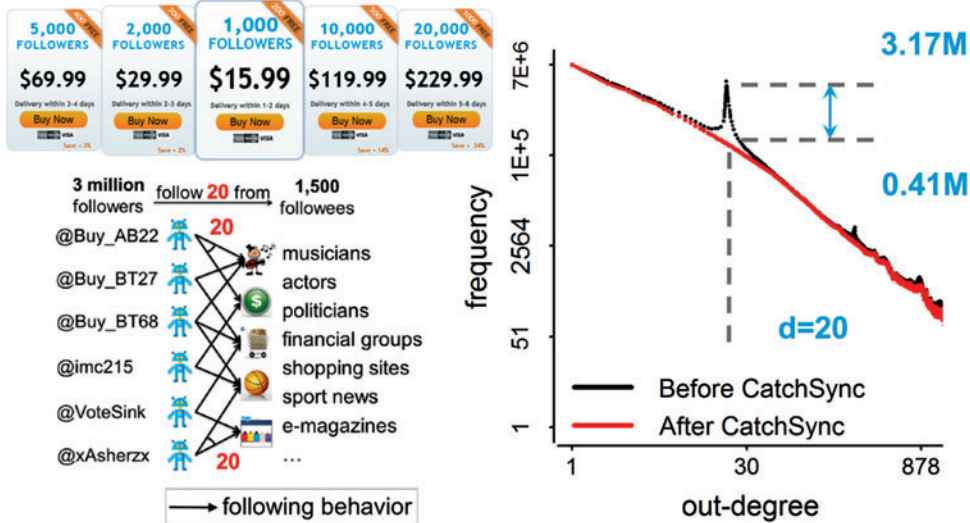
large percentage of spam, fraud, and Sybil attacks on popular platforms. Naturally, the owners of these platforms want to ensure that any behavior happening on them involves a real person interested in interacting with a specific Facebook page, following a specific Twitter account, or rating a specific Amazon product.

Many advanced SBD techniques have existed over the past 10 years, dividing suspicious behaviors into four categories: traditional spam, fake reviews, social spam, and link farming. Figure 6 shows the percentages of research works that focus on these categories. We can see tremendous progress in social spam detection and social link farming detection systems (Jiang et al. 2016b).

Link farming previously referred to a form of spamming on search engine indexes that connected all of a web page’s hyperlinks to every other page in a group. Today, it is grown to include many graph-based applications within millions of nodes and billions of edges. For example, in Twitter’s “who-follows-whom” graph, fraudsters are paid to make certain accounts seem more legitimate or famous by giving them additional followers (zombies). In Facebook’s “who-likes-what-page” graph, fraudsters create ill-gotten page likes to turn a profit from groups of users acting together, generally liking the same pages at around the same time (Beutel et al. 2013). Unlike spam content that can be caught via existing anti-spam techniques, link-farming fraudsters can easily avoid content-based detection: zombie followers do not have to post

suspicious content; they just distort the graph structure (Jiang et al. 2014c). Thus, the problem of combating link farming is rather challenging.

With a set of known spammers and a Twitter network, LockInfer uncovers lockstep behaviors in zombie followers and provides initialization scores by reading the social graph’s connectivity patterns (Jiang et al. 2014d, 2015b). CatchSync exploits two of the tell-tale signs left in graphs by fraudsters: they are often required to perform some task together and have “synchronized” behavioral patterns, meaning their patterns are rare and very different from the majority (Jiang et al. 2014c). Quantifying concepts and using a distance-based outlier detection method, CatchSync can achieve 0.751 accuracy in detecting zombie followers on Twitter and 0.694 accuracy on Tencent Weibo. CatchSync is complementary with content-based methods: combining content and behavioral information can improve accuracy by 6% and 9%, respectively. So far, as shown in Fig. 7, it has found three million suspicious users who connect to around 20 users from a set of 1,500 celebrity-like accounts on the 41-million-node Twitter network, creating a big spike on the out-degree distribution of the graph. Furthermore, removing the suspicious user nodes leaves a smooth power law distribution on the remaining part of the graph; strong evidence that recall on the full dataset is high. A scalable algorithm CrossSpot has been proposed to evaluate the suspiciousness of lockstep behaviors in multi-modal datasets (Jiang et al. 2015c).



**Behavior Modeling in Social Networks, Fig. 7** CatchSync has found three million suspicious users who connect to around 20 users from a set of 1,500 celebrity-like accounts on the 41-million-node Twitter

## Key Applications

The framework of behavior modeling supports multiple applications in social networks that can be categorized into two: predicting the “good” behaviors and detecting the “bad” behaviors.

### Behavior Prediction for Recommendation and Social Marketing

Recommender systems have become extremely common in a variety of social applications. The most popular systems are for movies, music, news, books, social tags, collaborators, restaurants, financial services, life insurance, friends, Twitter followers, and products in general.

Social media marketing connects these consumers and audiences to businesses that share the same needs, wants, and values. Precise behavior prediction techniques facilitate target advertising, product promotion, and online marketing in the social networks.

### Suspicious Behavior Detection

The popularity of social network sites has made them prime targets for spammers. Social spam is unwanted spam content appearing on OSNs with

network, creating a big spike on the out-degree distribution of the graph. Removing the suspicious user nodes leaves a smooth power law distribution on the remaining part of the graph; strong evidence that recall on the full dataset is high

UGC. It can be manifested in many ways, including bulk messages, profanity, insults, hate speech, malicious links, fraudulent reviews, fake friends, and personally identifiable information. Many of the social networks require an administrator’s time and energy to manually filter or remove spam. Automatic social spam detection is thus important.

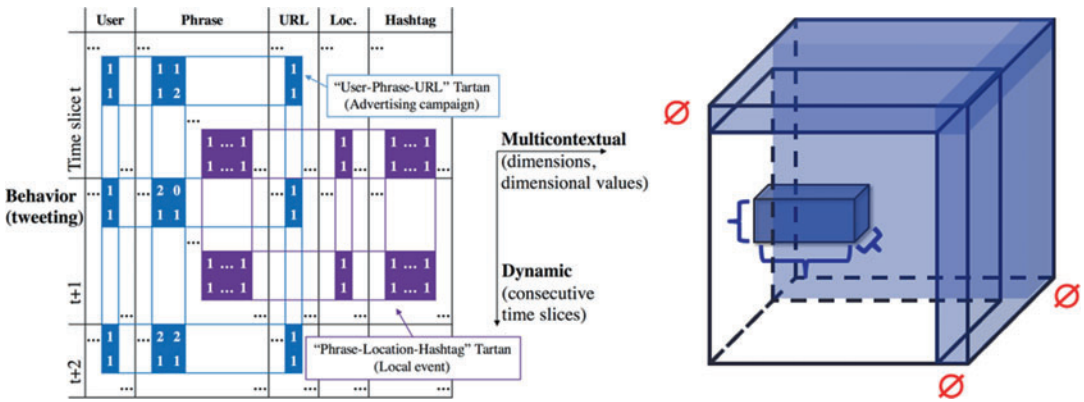
Besides social spam, the suspicious behaviors include fake reviews, fake comments, fake blogs, fake posts, and deceptive messages. Supervised learning, pattern discovery, graph-based methods, and relational modeling have been applied to address the problems in the real world. We also observe other typical suspicious behaviors such as ill-gotten Page Likes in Facebook, ill-gotten five stars in Amazon and eBay, and zombie followers in Twitter.

## Future Directions

### Modeling Aspect-Level Behavior Content

There is a big gap between existing behavior models and behavioral semantics. Integrating the context and content information requires





**Behavior Modeling in Social Networks, Fig. 8** Left: two-level matrix to represent multi-contextual behaviors; tartans to represent behavioral summaries. These

representations preserve more information from the behavioral data than standard matrix or tensor representations

comprehensive and accurate representations of the behavior content, and traditional bag of word (BOW) and LDA cannot well represent the rich content. The former one has a serious issue of sparseness. For example, “Mrs. Clinton” and “Hillary Clinton” often refer to the same celebrity, but the BOW regards them as different elements. The latter one is uninterpretable and the representations are too general. For example, the topical dimension of political words is too rough to understand the user’s response to the presidential election. Therefore, mining the entities and events, the attributes of and aspects related to the entities and events, and the users’ sentiments will facilitate the modeling of the behavior content and users’ intentions underlying the UGC.

**Modeling Multi-contextual and Dynamic Behaviors**

Traditional behavioral modeling represents a behavior as a tuple in which each element is one contextual factor of one type, and the tensor-based summaries look for high-order dense blocks by clustering the values (including time stamps) in each dimension. However, Fig. 8 shows that the human behaviors are multi-contextual and dynamic: (1) each behavior takes place within multiple contexts in a few dimensions, which requires the representation to enable non-value and set values for each dimension; (2) many behavior collections, such as tweets or papers,

evolve over time. An idea is to represent the behavioral data as a two-level matrix (temporal behaviors by dimensional values) and to represent behavioral summary as tartans that includes a set of dimensions, the values in each dimension, a list of consecutive time slices, and the behaviors in each slice. As in Fig. 8, these representations preserve more information from the behavioral data than standard matrix or tensor representations. How to develop prediction and detection techniques on the new representations is important for multi-contextual behavior modeling.

**Modeling the Causal Effects of Behaviors**

Coming to the big data era, statistical modeling, which is a powerful tool for developing and testing theories by way of causal explanation, prediction, and description, has been adopted in a broad range of applications. For example, in online advertising, causal model was used to explain the causal effect of advertising strategies, and in information propagation, predictive model was employed for cascading outbreak detection (Cui et al. 2013). Usually there are two important aspects of statistical modeling: prediction performance and model interpretability. A good model should be both predictive and interpretable. Causal inference, which refers to the process of drawing a conclusion about a causal connection based on the conditions of the occurrence of an effect (Holland 1986), is a powerful statistical

modeling tool for explanatory analysis. It is usually believed that models with high explanatory power are inherently of high predictive power (Shmueli 2010).

### Other Future Directions

Back to Fig. 1, behavior modeling is designed to serve both the industrial and research communities. For industry, *applied behavior modeling* refers to (1) extend the scalability and parallelizability of the algorithms in online applications and (2) conduct online testing experiments to demonstrate the effectiveness of the algorithms. For scientific research, traditional discoveries were generated from a small series of experiments due to the high cost of human labor. Now with the large-scale databases of social networks, how to use *behavior modeling results to benefit social and behavioral sciences* becomes important.

### Cross-References

- ▶ [Behavior Analysis in Social Networks](#)
- ▶ [Human Behavior and Social Networks](#)
- ▶ [Recommender Systems: Models and Techniques](#)
- ▶ [Social-Based Collaborative Filtering](#)
- ▶ [Spam Detection on Social Networks](#)
- ▶ [User Behavior in Online Social Networks, Influencing Factors](#)

### References

- Balabanović M, Shoham Y (1997) Fab: content-based, collaborative recommendation. *Commun ACM* 40(3):66–72
- Beutel A, Xu W, Guruswami V, Palow C, Faloutsos C (2013) Copycatch: stopping group attacks by spotting lockstep behavior in social networks. In: Proceedings of the 22nd international conference on World Wide Web, Rio de Janeiro, pp 119–130, 13–17 May 2013
- Blei DM, Ng AY, Jordan MI (2003) Latent dirichlet allocation. *J Mach Learn Res* 3:993–1022
- Bond R, Smith PB (1996) Culture and conformity: a meta-analysis of studies using asch's (1952b, 1956) line judgment task. *Psychol Bull* 119(1):111
- Chirita PA, Diederich J, Nejdil W (2005) MailRank: using ranking for spam detection. In: Proceedings of the 14th ACM international conference on Information and knowledge management, Bremen, 31 Oct–5 Nov 2005, pp 373–380
- Cui P, Jin S, Yu L, Wang F, Zhu W, Yang S (2013) Cascading outbreak prediction in networks: a data-driven approach. In: Proceedings of the 19th ACM SIGKDD international conference on knowledge discovery and data mining, Chicago, 11–14 Aug 2013, pp 901–909
- Holland PW (1986) Statistics and causal inference. *J Am Stat Assoc* 81(396):945–960
- Jiang M, Cui P, Wang F, Yang Q, Zhu W, Yang S (2012a) Social recommendation across multiple relational domains. In: Proceedings of ACM international Conference on information and knowledge management (CIKM), Maui, 29 Oct–2 Nov 2012, pp 1422–1431
- Jiang M, Cui P, Liu R, Yang Q, Wang F, Zhu W, Yang S (2012b) Social contextual recommendation. In: Proceedings of ACM international conference on information and knowledge management (CIKM), Maui, 29 Oct–2 Nov 2012, pp 45–54
- Jiang M, Cui P, Wang F, Xu X, Zhu W, Yang S (2014a) FEMA: flexible evolutionary multi-faceted analysis for dynamic behavioral pattern discovery. In: Proceedings of ACM SIGKDD international conference on knowledge discovery and data mining (SIGKDD), New York, 24–27 Aug 2014, pp 1186–1195
- Jiang M, Cui P, Wang F, Zhu W, Yang S (2014b) Scalable recommendation with social contextual information. *IEEE Trans Knowl Data Eng (TKDE)* 26(11):2789–2802
- Jiang M, Cui P, Beutel A, Faloutsos C, Yang S (2014c) CatchSync: catching synchronized behavior in large directed graphs. In: The 20th ACM SIGKDD international conference on knowledge discovery and data mining (KDD), New York, 24–27 Aug 2014, pp 941–950
- Jiang M, Cui P, Beutel A, Faloutsos C, Yang S (2014d) Inferring strange behavior from connectivity pattern in social networks. In: Proceedings of the 18th Pacific-Asia conference on knowledge discovery and data mining (PAKDD), Tainan, 13–16 May 2014, pp 126–138
- Jiang M, Cui P, Chen X, Wang F, Zhu W, Yang S (2015a) Social recommendation with cross-domain transferable knowledge. *IEEE Trans Knowl Data Eng* 27(11):3084–3097
- Jiang M, Beutel A, Cui P, Hooi B, Yang S, Faloutsos C (2015c) A general suspiciousness metric for dense blocks in multimodal data. In: The 15th IEEE International Conference on Data Mining (ICDM)
- Jiang M, Cui P, Yuan NJ, Xie X, Yang S (2016a) Little is much: bridging cross-platform behaviors through overlapped crowds. In: Proceedings of the thirtieth AAAI conference on artificial intelligence, Phoenix, 12–17 Feb 2016, pp 13–19
- Jiang M, Cui P, Faloutsos C (2016b) Suspicious behavior detection: current trends and future directions. *Intell Syst IEEE* 31(1):31–39

- Jiang M, Cui P, Beutel A, Faloutsos C, Yang S (2016c) Inferring lockstep behavior from connectivity pattern in large graphs. *Knowl Inf Syst* 48(2):399–428
- Koren Y (2008) Factorization meets the neighborhood: a multifaceted collaborative filtering model. In: *Proceedings of the 14th ACM SIGKDD international conference on knowledge discovery and data mining*, Las Vegas, 24–27 Aug 2008. ACM, New York, pp 426–434. ISBN:978-1-60558-193-4
- Koren Y (2010) Collaborative filtering with temporal dynamics. *Commun ACM* 53(4):89–97
- Koren Y, Bell R, Volinsky C (2009) Matrix factorization techniques for recommender systems. *Computer* 8:30–37
- Li B, Yang Q, Xue (2009) Can movies and books collaborate? Cross-domain collaborative filtering for sparsity reduction. Hong Kong, China, *IJCAI* 9:2052–2057. ISBN: 978-1-60558-512-3
- Liben-Nowell D, Kleinberg J (2007) The link-prediction problem for social networks. *J Am Soc Inf Sci Technol* 58(7):1019–1031
- Liu X, Aberer K (2013) Soco: a social network aided context-aware recommender system. In: *Proceedings of the 22<sup>nd</sup> international conference on World Wide Web*, Rio de Janeiro, 13–17 May 2013, pp 781–802
- Liu NN, Zhao M, Yang Q (2009) Probabilistic latent preference analysis for collaborative filtering. *Proceedings of the 18th ACM conference on Information and knowledge management*, Hong Kong, 2–6 Nov 2009. ACM, New York, pp 759–766. ISBN:978-1-60558-512-3
- Liu Q, Chen E, Xiong H et al (2012) Enhancing collaborative filtering by user interest expansion via personalized ranking. *Syst Man Cybern Part B Cybern IEEE Trans* 42(1):218–233
- Narang K, Nagar S, Mehta S et al (2013) Discovery and analysis of evolving topical social discussions on unstructured microblogs. In: *Proceedings of the 35th European conference on advances in information retrieval*, Moscow, 24–27 Mar 2013. Springer, Berlin/Heidelberg, pp 545–556. ISBN:978-3-642-36972-8
- Sarwar B, Karypis G, Konstan J et al (2001) Item-based collaborative filtering recommendation algorithms. *Proceedings of the 10th international conference on World Wide Web*, Hong Kong, 1–5 May 2001. ACM, New York, pp 285–295. ISBN:1-58113-348-0
- Schilit B, Adams N, Want R (1994) Context-aware computing applications. *Proceedings of the 1994 first workshop on mobile computing systems and applications*, 8–9 Dec 1994, pp 85–90
- Shmueli G (2010) To explain or to predict? *Stat Sci* 25(3):289–310. doi:10.1214/10-STS330
- Tang J, Hu X, Gao H et al (2013) Exploiting local and global social context for recommendation. *Proceedings of the twenty-third international joint conference on artificial intelligence*, Beijing, 3–9 Aug 2013. AAAI Press, pp 2712–2718. ISBN:978-1-57735-633-2
- Xu Q, Xiang EW, Yang Q, Du J, Zhong J (2012) Sms spam detection using noncontent features. *IEEE Intell Syst* 27(6):44–51
- Yuan Q, Cong G, Ma Z, Sun A, Thalmann NM (2013) Who, where, when and what: discover spatio-temporal topics for twitter users. In: *Proceedings of the 19th ACM SIGKDD international conference on knowledge discovery and data mining*, Chicago, 11–14 Aug 2013. ACM, New York, pp 605–613. ISBN:978-1-4503-2174-7
- Zhong E, Fan W, Yang Q (2014) User behavior learning and transfer in composite social networks. *ACM TKDD* 8(1):6