TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 04/09 pp734–742
DOI: 10.26599/TST.2020.9010005
Volume 25, Number 6, December 2020

A Survey of Game Theory as Applied to Social Networks

Xinfang Song, Wei Jiang*, Xiaohui Liu, Hui Lu*, Zhihong Tian, and Xiaojiang Du

Abstract: Social network services can not only help people form relationships and make new friends and partners, but also assist in processing personal information, sharing knowledge, and managing social relationships. Social networks achieve valuable communication and collaboration, bring additional business opportunities, and have great social value. Research on social network problems is effective by using assumption, definition, analysis, modeling, and optimization strategies. In this paper, we survey the existing problems of game theory applied to social networks and classify their application scenarios into four categories: information diffusion, behavior analysis, community detection, and information security. Readers can clearly master knowledge application in every category. Finally, we discuss certain limitations of game theory on the basis of research in recent years and propose future directions of social network research.

Key words: social network; social value; application scenarios; game theory

1 Introduction

With the development of science and technology, social networks have become an essential portion of human daily life and have attracted great research interest in different fields. Social networks are a kind of multidimensional space — based on relationship chains — that have strong diffusion and involve various interactive behaviors. The purpose is to provide various relationships and exchange interaction pathways to users[1–3]. Social networks blur the virtual world and reality; users in social networks can identify information and statuses, make friends, upload photographs and small videos from their lives, attract other people to see something interesting, and share funny things with other people. In addition, users can filter and integrate huge amounts of information on the internet through attention and subscription. Social network has experienced four developingt processes: (1) the early conceptualization stage—six degree separation theory, represented by SixDegrees; (2) the stage of making friends with strangers , e.g., Friendster helps you build weak relationships and bring higher social capital; (3) the stage of entertainment, e.g., MySpace creates rich multimedia personalized space to attract attention; and (4) the stage of social graph, e.g., Facebook replicates the theory of online low-cost management from offline real networks. Therefore, each stage hugely contributes to later scholars. Today's social network research is related to physics, biology, social science, network technology, engineering, and other fields.

Grofman and Owen[4] put forward research applying game theory to social networks. The current research problem of game theory has been divided into different kinds by diverse conditions: (1) by the number of participants: two-player, three-player, and multi-player games[5–10]; (2) by the payoffs of players: zero-, constant-, and variable-sum games; (3) by the order of players: static and dynamic games; (4) by the construction of information: complete and incomplete

• Xinfang Song and Xiaohui Liu are with Beijing Information Technology College, Beijing 100015, China. E-mail: songxf@bitc.edu.cn; liuxiaohui@bitc.edu.cn.
• Wei Jiang is with Chinese Academy of Cyberspace Studies, Beijing 100010, China. E-mail: jw@bjut.edu.cn.
• Hui Lu and Zhihong Tian are with Guangzhou University, Guangzhou 510006, China. E-mail: luhui@gzhu.edu.cn; tianzhihong@gzhu.edu.cn.
• Xiaojiang Du is with the Department of Computer and Information Sciences, Temple University, Philadelphia, AZ 19122, USA. E-mail: dxj@ieee.org.
∗ To whom correspondence should be addressed.
Manuscript received: 2020-01-27; accepted: 2020-02-05

information games; (5) by the profile of players: cooperative and non-cooperative games; and (6) by the rationality of players: rational and irrational games.

The weakness of the traditional social network approach is it lacks dynamic interaction. To this end, game theory is recommended for analyzing different scenarios. Through the algorithm, models and empirical methods analyze players, actions, strategies, payoffs, equilibria, and results. These factors portray the game model and put forward the profit function of each player. Considering the game model and real human behaviors, we summarize the optimization strategy. The paper is organized in the following manner. Section 2 discusses game theory, social network, and evaluates game theory application methods in different ways, such as information diffusion, community detection, behavior analysis, and information security, by collecting research results. Section 3 proposes future research directions on the basis of recent limitations. Section 4 summarizes the paper. This review aims to help scholars quickly acknowledge game theory applications in social networks; researchers can reference certain suggestions from this paper for further research.

2 Classification of Game Theory Applications in Social Networks

Most game theory applications in social network research are about individuals' behaviors and the strategic interactions among these individuals. Most previous researchers first analyzed the problem, and then created a game theory model. The game-theoretic model describes each node as a selfish node, which can choose its motivation for increasing its own revenue, and the state is the game strategy. The model properly captures individuals' natural strategies and describes social networks' state. Different directions exist for further exploration, we can obtain excellent models and methods by reviewing various aspects of social networks in different studies through collection, sorting, analysis, and induction. Based on the literature review, we present a taxonomy for classifying research fields in Fig. 1, which provides a global view of the social network problem to scholars.

2.1 Application for information diffusion

In the social network analysis, most users are defined as nodes. The relationship among individuals can be abstractly represented using the edges between the corresponding nodes in which the data are spread along the edges. Regarding information diffusion and influence, we can analyze individuals, groups, and relationships among groups. We perform information diffusion under the influence of various factors, such as relationship between users, network topology, users' psychology, knowledge, and feedback transfer. In game theory applications, people on both sides of a game can be considered individuals from each other or individuals from their neighbors to analyze information diffusion in social networks. From rational and irrational factors, we analyze their states when transmitting messages, information dissemination costs and revenues, and optimization strategies.

Graphics, matrices, and statistics can be used during analysis, of which the most used are mathematical formulas or abstract theories. Certain researchers collected and analyzed large amounts of information from social networks; formed theoretical analyses for actual analyses, thus obtaining certain regularities among them; and confirmed the correctness of the proposed models and algorithms.

Several recent studies have emphasized the issue of information diffusion[5,11]. Reiffers-Masson et al.[5] presented a model of the competition among sources by using a non-cooperative game. Huang et al.[6] adopted the empirical method to gather information from Twitter. They modeled a diagrammatic match to simulate the

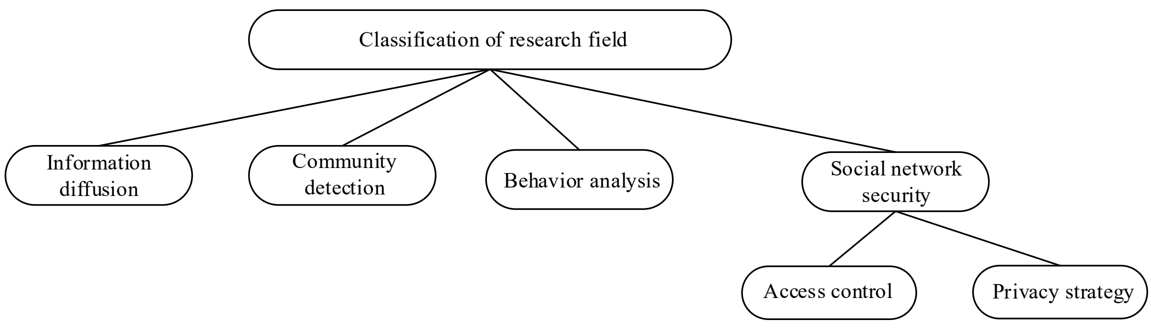


Fig. 1 Classification of research filed.

system for easy analysis. The information diffusion diagram is shown in Fig. 2.

In Fig. 2, the five nodes represent the five users, and the edges between the nodes represent news that can be shared between them. By taking the threshold as 5, valuations of Players 1, 2, 3, 4, and 5 are 7, 6, 4, 2, and 1, respectively. Letting Player 1 be the first message originator, communicators can only be 2 and 3. We can see this situation in Fig. 2a. A strategy is then proposed to increase the valuations of other players and enrich the original message by adding comments and related information. Thus, Player 3 joins the diffusion process, as illustrated in Fig. 2b. Through this basic model, the game process is abstracted, and players' strategies and benefits are analyzed. An algorithm is also proposed to find Nash equilibrium solutions and provide numerical examples.

All players' strategies are derived. In their solution in Table 1, v_i represents players' valuations to the original information; s_i indicates players' strategy profile; and u_i is players' utility function, which is based on the limbic rise cost; as the growing strive exists, players regard it as earnings. Table 1 provides the instance of certain players playing the strategies of Nash equilibrium by giving system arguments to prove the system's stability. Finally, high valuation users are willing to strongly strive to enrich the original information. The above analysis uses an empirical method and a graphic game, but does not consider users' decision, motivation, cognition, attitude, emotion, and social financial connections, which are usually neglected by existing works in the network. Jiang et al.[11] considered the diffusion system's analysis based on network modeling, empirical approaching, data mining, and a user's action. The authors proposed an evolutionary game-theoretic framework applied to the dynamic information diffusion process in social networks.

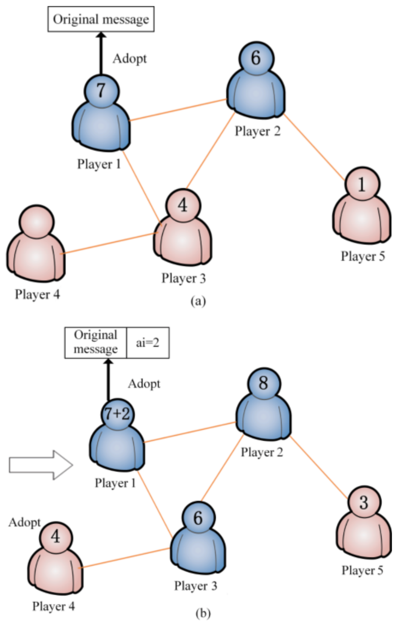


Fig. 2 Diagrammatic figure of the system[6].

Table 1 Numerical result for complete network.

ID	v_i	s_i	u_i
Player 1	60.0000	2.4002, adopt	90.6223
Player 2	30.0000	1.7071, adopt	45.3109
Player 3	15.0000	1.0139, adopt	22.6556
Player 4	7.5000	0.3208, adopt	11.3277
Player 5	3.7500	0, adopt	5.3530
Player 6	1.8750	0, adopt	2.1765
Player 7	0.9375	0, adopt	0.5882
Player 8	0.4688	Ignore	0

2.2 Application for community detection

Another common network property of social networks is community structure characteristics. That is, internal connections between nodes bring communities close, whereas connections between communities are relatively sparse. Communities are groups of people who have common characteristics; for example, organizations, groups of people with the same hobby, and company departments. The community detection algorithm can make effective detections about how people's activities and interactions affect the dynamic social network. By analyzing the dynamic game theory of social networks, we can naturally find communities in social networks, learn their structure, find optimization community models, analyze relationships between communities, provide valuable information in networks, and prevent potential safety problems, such as spread of viruses and worms.

A popular problem in social networks is community detection[12–16] . Jiang and Xu[17] referenced a graph[18] about the distribution of degrees in diverse communities. According to the analysis, gain, loss, and utility functions are based on intelligent and selfish actions, such as joining or leaving communities. In Fig. 3, three correlative communities indicated by A, B, and C are defined. Node v is the node of interest, and its gain and loss functions are analyzed.

An intelligent and selfish agent options for a set of actions — joining or leaving communities — to maximize its utility. A dynamic network is considered to be a sequence of snapshots. Each snapshot has

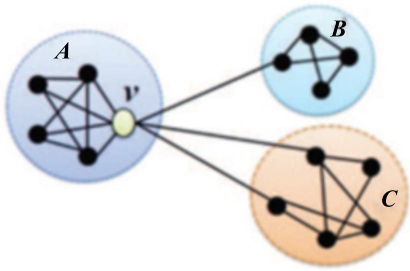


Fig. 3 Model distribution of small communities[17].

its community result. Through the analysis, the corresponding algorithm is proposed. Although the community structure can be smoothly detected by its dynamic community detection game over time, only the game with pure strategy is discussed, and each community is restricted as non-overlapping. Investigating overlapping cases is challenging. Chen et al.[19] proposed a new valid method of signed network community partition on the basis of game theory. Yu et al.[20] introduced a game-theoretic approach that identifies interaction groups in social networks. Most analyses are based on an algorithm and model. Therefore, a huge gap remains between realistic and expected behaviors.

2.3 Application for behavior analysis

User behavior in social networks is a kind of dynamic interaction, which constantly evolves during the whole development process. The interaction behaviors of users reflect the main features of social networks. Over the past few years, many scholars have made great contributions to this research field.

(1) Identify node properties, explore social network secret nodes, determine influential individuals for viral marketing, and explore node centricity. In complex social networks, exploring secret nodes is important; doing so may help timely perceive terrorists, recommend certain items to possible customers, and find sources of rumors. Given these factors, we can easily and effectively control the condition of social networks. Yang et al.[21] discovered covert nodes in social networks. According to the influence transmission base on the model, they identified the strategy user {infected, normal} strategy influential {overt, convert}. Subsequently, they derived the pay-off matrix, as presented in Table 2.

Table 2 Pay-off matrix[21].

User	Influential	
	Overt	Convert
Infected	$U_{\text{user}}(i,o)$, $U_{\text{influential}}(i,o)$	$U_{\text{user}}(i,c)$, $U_{\text{influential}}(i,c)$
Normal	$U_{\text{user}}(n,o)$, $U_{\text{influential}}(n,o)$	$U_{\text{user}}(n,c)$, $U_{\text{influential}}(n,c)$

In their model, the users are divided into normal and infected nodes. The influential node has two states: overt or convert. According to Bayes theorem, they obtained the related parameters and calculated the nodes earning on real and simulation datasets. The method that they used is verified. Improving the quality of the services offered via these networks is possible by identifying the crucial components in the network. Aadithya and Ravindran[22] developed analytical formulas for computing the Shapley node values for all kinds of centrality-related cooperative games played on weighted and unweighted networks. These formulas provide valid and error-free methods of computing node centralities. However, their surprisingly simple closed form expressions also offer intuition about why certain nodes are relatively important to networks. In the model of Ref. [23], the influence game can capture players' interactions and behaviors, and the algorithm can identify most influence nodes in social networks.

(2) The two features of social networks are scale-free and small-world, which are based on the formation of small-world networks. Yang and Chen[24] presented a game-theoretic model and a network formation as a game in which people search for long-distance and high reciprocity relationships. Importantly, they provided significantly new insights into the connections between distance, reciprocity, and navigability in social networks. The topology model can naturally be expressed in the interior structure of many games in real environments. The diagrammatic players set their decisions on the basis of the influences of nearby people. Rajtmajer et al.[25] made the first effort to investigate evolutionary game models to explain the spread of cyber violence. They formulated a game by using two strategies where each player's behavior is classified as normal (cooperate) or abusive (defect). Through the empirical measurements of the model against a real-world dataset collected from the web, they provided a visualized network graph and the corresponding degree distribution, which follows the representative power-law model.

Figure 4 includes 62 060 posts over 787 threads, and a network of 2586 individual nodes (users) is obtained. These nodes are connected by 62 931 unweighted, undirected edges. Figure 5 reflects the distribution of node degrees.

In this study, a single pay-off matrix among all users is proposed. Further research may involve multiple pay-off matrices, which can indicate users' anomalous

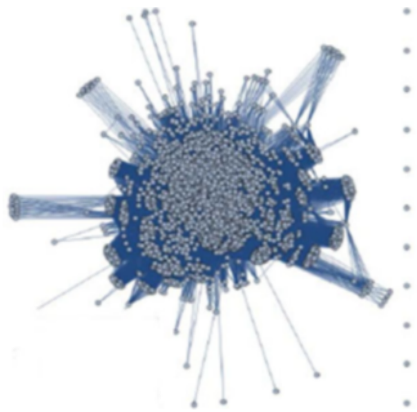


Fig. 4 Network graph[25].

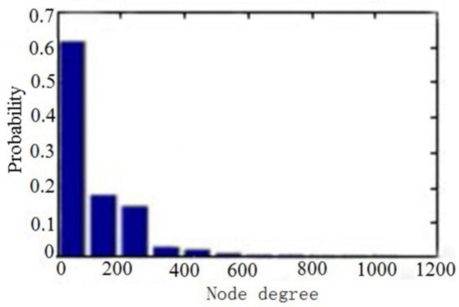


Fig. 5 Distribution of node degrees[25].

actions and analyze different pay-off schemes. Kearns et al.[26] proposed a multi-player game consisting of n players, each with a finite set of pure strategies or actions available to them, along with a specification of the payoffs to each player. Subsequently, they built a Markov network, which represents all related equilibria of the graphical game that portrays pay-off equivalence and provides a general algorithm for computing correlated equilibria.

2.4 Application for social network security

Social networks have large user groups and large amounts of information, which has attracted the attention of many invaders. The safety of social networks should not be ignored. Common security issues include the disclosure of users' privacy information, loss of property, attack from rogue software, and opening of unsafe links. Game theory applications in social networks involve establishing user trust mechanisms, simulating network control managers' activities, controlling access, analyzing privacy, and putting forward reasonable privacy management strategies. Game theory issues are applied to network security; most ordinary users of social networks and network attackers can be on both sides of the game. Various strategies for profits are analyzed, and the results are tested in the simulation system[7,8,27,28]. Research on information security in the social network field is abundant.

(1) Access control

Access control can effectively guarantee network security. Many scholars realize research on access control in social networks through the game model. Squicciarini et al.[29] adopted the two-user game model to solve the user authentication problem within registered social networks. They were the first to develop an analytical model to study the dynamics underpinning user registration in social media. Lin et al.[30] applied the game theory in fingerprint identification for the multimedia of social network software. Hu et al.[31] focused on the problem of online social networks where only a single user is allowed to restrict access to her/his data but cannot provide any mechanism to enforce privacy concerns over data associated with multiple users. This relationship is shown in Fig. 6.

Circles are used to represent the accessor spaces of three controllers of a shared data item, c_1, c_2, and c_3. The segment is divided into two parts: non-conflicting and conflicting. Segment ns is non-conflicting, whereas cs_1 through cs_6 are conflicting segments. cs_1, cs_2, and cs_3 each indicates one privacy conflict; and cs_4, cs_5, and cs_6 are associated with two privacy conflicts. Through the game model and considering that controllers may attempt to selfishly maximize their own profits, a multi-party access control model is proposed. The multi-party control game is analyzed using an adjustment algorithm and a numerical analysis based on three different situations with respect to the numbers of untrusted accessors (μ) and trusted accessors (τ) in conflicting segments.

Azadjalal et al.[32] proposed an awareness recommendation system on the basis of a novel trust by combining the Pareto dominance concept and

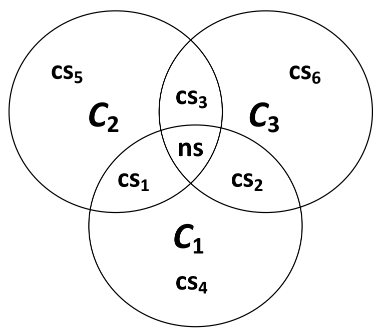


Fig. 6 Privacy conflict identification[31].

social networks.

(2) Privacy strategy

Game theory method can fully consider the interests of parties, which include the user and the attacker. We propose a solution which makes such interests safe and balances the relationship between privacy and service quality in solving the problem of privacy strategy. Chen et al.[28] researched users' profile attribute disclosure behaviors. Specifically, they modeled the privacy and set dynamics of social networks by using three game-theoretic approaches.

Two-user game refers to basic and weighted evolutionary games. The three models reflect the influence of different factors on users' privacy choices. White et al.[27] presented a novel Online Social Networks (OSN) modeling approach, which is based on an innovative game theoretical approach to analyze certain different attack scenarios. Different from the other model, the analysis considers whether the attacker is allowed to have different motivations and different amounts of knowledge about the underlying system. In the discussion, game states are shared, masked, concealed, and exposed. The model helps users determine the optimal policy for data sharing on OSNs, which use a Markov game model. Squicciarini et al.[29] also investigated privacy issues with shared content in social network sites. They used the Clarke Tax mechanism to present a theoretical representation of the collective privacy management problem and proposed a solution that builds upon well-known game theoretical results. They were the first to propose a privacy protection mechanism for social networking.

3 Future Research Direction

By integrating game theory with economics, operational research, and computer science methods can well satisfy the analyses of social network issues and user behavior characterizations[33,34]. On one hand, scholars put forward a formula and an algorithm that can be used to analyze the game problem. On the other hand, participants' various game behaviors can be captured in social networks. In this section, based on the shortcomings of current game-theoretic approaches, we propose future research directions.

(1) The most suitable game model and profit function must be selected. When researchers portray different game models in their analysis, they should accurately map definitions in each model. Models lack full theoretical analyses. Other problems include the lack of interactivity, and how to extract the preferences of participants choose suitable models and profit functions. The game theory aspect is not confined to two or three sides. Parties can compile spatial locations on game simulations to show the trend of different strategy combinations and obtain the corresponding analysis results.

(2) Although game theory can bring the virtual world close to reality, fully considering various factors to make future theoretical analyses realistic is important. Most recent research focus on mathematical formulas or abstract theories, which may cause gaps with reality. Model factors greatly influence the accuracy of problem analyses. Conclusions may become different after considering plus factors. For example, future research can consider all directions, such as the psychological characteristic, interaction length, emotional vulnerability, intimate degree of users, and the diversity of the interactive content. Roles vary depending on different situations; identification in reality is difficult. Users may be normal in one community, but illegal in another community. The effective combination of the virtual world and reality must be improved.

(3) The accuracy of the sample data analysis must be improved. Preprocessing is necessary before conducting several user information data analyses. By removing users with an abnormal behavior, we can obtain accurate results.

(4) Multiple platforms and additional samples can be used for future theoretical research[35,36]. When we use game theory to analyze social network issues, we analyze the obtained information on social software. Multiple platforms and others samples should also be considered to verify analysis.

4 Conclusion

This study conducts a survey of social network analysis according to the game theory method. Game theory models can best capture the natural strategies of individuals and describe the state of social networks. In our research, the application area is divided into four parts: information diffusion, community detection, behavior analysis, and information security. We present future research directions through a comprehensive analysis. From this review, readers can further understand game theory applications in social networks and future directions to help improve such applications.

Acknowledgment

The paper was supported by the Natural Science Foundation of Beijing (No. 4172006), the Guangdong Province Key Area R&D Program of China (No. 2019B010137004), the National Natural Science Foundation of China (Nos. U1636215, 61972108, and 61871140), the National Key Research and Development Plan (No. 2018YFB0803504), and Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019).

References

[1] J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city, *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2019.2943906.

[2] L. Yin, X. Luo, C. Zhu, L. Wang, Z. Xu, and H. Lu, ConnSpoiler: Disrupting C&C communication of IoT-based botnet through fast detection of anomalous domain queries, *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2019.2940742.

[3] W. Jiang, M. Gao, X. Wang, and X. Wu, A new evaluation algorithm for the influence of user in social network, *China Communications*, no. 2, pp. 200–206, 2016.

[4] B. Grofman and G. Owen, A game theoretic approach to measuring degree of centrality in social networks, *Social Networks*, vol. 4, no. 3, pp. 213–224. 1982.

[5] A. Reiffers-Masson, Y. Hayel, and E. Altman, Game theory approach for modeling competition over visibility on social networks, in *Proc. of Sixth International Conference on Communication Systems & Networks*, Bangalore, India, 2014, pp. 1–6.

[6] J. Huang, C. Wang, and H. Wei, Strategic information diffusion through online social networks, in *Proc. of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, Barcelona, Spain, 2011, pp. 26–29.

[7] W. Jiang, B. Fang, Z. Tian, and H. Zhang, Research on defense strategies selection based on attack-defense stochastic game model, *Journal of Computer Research and Development*, vol. 47, no. 10, pp. 1714–1723, 2010.

[8] W. Jiang, B. Fang, Z. Tian, and H. Zhang, Evaluating network security and optimal active defense based on attack-defense game model, *Chinese Journal of Computers*, vol. 32, no. 4, pp. 817–827, 2009.

[9] Z. Tian, X. Gao, S. Su, and J. Qiu, Vcash: A novel reputation framework for identifying denial of traffic service in internet of connected vehicles, *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2019.2951620.

[10] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, A distributed deep learning system for web attack detection on edge devices, *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, 2019.

[11] C. Jiang, Y. Chen, and K. Liu, Evolutionary social information diffusion analysis, in *Proc. 2014 IEEE Global Communications Conference*, Austin, TX, USA, 2014, pp. 2911–2916.

[12] R. Lung, C. Chira, and A. Andreica, Game theory and extremal optimization for community detection in complex dynamic networks, *PloS One*, vol. 9, no. 2, p. e86891, 2014.

[13] M. Shokmezhad and S. Khorsandi, Joint power control and channel assignment in uplink to network: A noncooperative game and auction based approach, *Computer Communications*, vol. 118, no. 3, pp. 1–13, 2018.

[14] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, A distributed deep learning system for web attack detection on edge devices, *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2019.2938778.

[15] L. Xiao, Y. Li, X. Huang, and X. Du, Cloud-based malware detection game for mobile devices with offloading, *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2742–2750, 2017.

[16] Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su, Y. Sun, and N. Guizani, Real time lateral movement detection based on evidence reasoning network for edge computing environment, *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4285–4294, 2019.

[17] F. Jiang and J. Xu, Dynamic community detection based on game theory in social networks, in *Proc. of 2015 IEEE International Conference on Big Data*, Santa Clara, CA, USA, 2015, pp. 2368–2373.

[18] T. Chakraborty, S. Srinivasan, N. Ganguly, A. Mukherjee, and S. Bhowmick, On the permanence of vertices in network communities, in *Proc. of the 20th ACM International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA, pp. 1396–1405, 2014.

[19] X. Chen, X. Du, J. Yu, J. Guo, Z. Cui, and L. Fu, Research of community mining in signed social network based on game theory, *International Journal of Innovative Computing, Information and Control*, vol. 10, no. 6, pp. 2221–2235, 2014.

[20] J. Yu, Y. Wang, X. Jin, and X. Chen, Identifying interaction groups in social network using a game-theoretic approach, in *Proc. of the 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies*, Washington, DC, USA, 2014, pp. 511–518.

[21] A. Yang, Y. Tang, J. Wang, and J. Chen, Covert nodes mining in social networks based on games theory, in *Proc. of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design*, Hsinchu, China, 2014, pp. 541–545.

[22] K. Aadithya and B. Ravindran, Game theoretic network centrality: Exact formulas and efficient algorithms, in *Proc. of the 9th International Conference on Autonomous Agents and Multiagent Systems*, Toronto, Canada, 2010, pp. 1459–1460.

[23] M. Irfan and L. Ortiz, A game-theoretic approach to influence in networks, in *Proc. of the Twenty-Fifth AAAI Conference on Artificial Intelligence*, San Francisco, CA, USA, 2011, pp. 688–694.

[24] Z. Yang and W. Chen, A game theoretic model for the

formation of navigable small-world networks, in *Proc. of the 24th International Conference on World Wide Web*, Florence, Italy, 2015, pp. 1329–1339.

[25] S. Rajtmajer, C. Griffin, D. Mikesell, and A. Squicciarin, An evolutionary game model for the spread of non-cooperative behavior in online social networks, in *Proc. of the 30th Annual ACM Symposium on Applied Computing*, New York, NY, USA, 2015, pp. 1154–1159.

[26] M. Kearns, M. Littman, and S. Singh, Graphical models for game theory, in *Proc. of the Seventeenth Conference on Uncertainty in Artificial Intelligence*, San Francisco, CA, USA, 2001, pp. 253–260.

[27] J. White, J. Park, C. Kamhoua, and K. Kwiat, Game theoretic attack analysis in online social network (OSN) services, in *Proc. of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Niagara, Canada, 2013, pp. 1012–1019.

[28] J. Chen, M. Brust, A. Kiremire, and V. Phoha, Modeling privacy settings of an online social network from a gametheoretical perspective, in *Proc. of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, TX, USA, 2013, pp. 213–220.

[29] A. Squicciarini, C. Griffin, and S. Sundareswaran, Towards a game theoretical model for identity validation in social network sites, in *Proc. of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, Boston, MA, USA, 2011, pp. 1081–1088.

[30] W. Lin, H. Zhao, and K. Liu, Game-theoretic strategies and equilibriums in multimedia fingerprinting social networks, *IEEE Transactions on Multimedia*, vol. 13, no. 2, pp. 191–205, 2011.

[31] H. Hu, G. J. Ahn, Z. Zhao, and D. Yang, Game theoretic analysis of multiparty access control in online social networks, in *Proc. of the 19th ACM Symposium on Access Control Models and Technologies*, London, Canada, 2014, pp, 93–102.

[32] M. Azadjalal, P. Moradi, and A. Abdollahpouri, Application of game theory techniques for improving trust-based recommender systems in social networks, in *Proc. of 4th International Conference on Computer and Knowledge Engineering*, Mashhad, Iran, 2014, pp. 261–266.

[33] M. Shen, B. Ma, L. Zhu, R. Mijumbi, X. Du, and J. Hu, Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection, *IEEE Transactions on Information Forensics & Security*, vol. 13, no. 4, pp. 940–953, 2018.

[34] P. Dong, X. Du, H. Zhang, and T. Xu, A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows, in *Proc. of IEEE International Conference on Communications*, Kuala Lumpur, Malaysia, 2016, pp. 1–6.

[35] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, Security in mobile edge caching with reinforcement learning, *IEEE Wireless Communications*, vol. 25, no. 3, pp. 116–122, 2018.

[36] L. Wu, X. Du, W. Wang, and B. Lin, An out-of-band authentication scheme for internet of things using blockchain technology, in *Proc. of 2018 International Conference on Computing, Networking and Communications*, Maui, HI, USA, 2018, pp. 769–773.

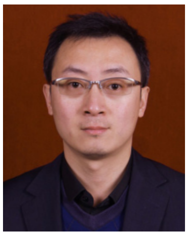
Xinfang Song received the MS degree from Harbin Normal University, China in 2007. She is an associate professor at Beijing Information Technology College. Her research interests include Lie algebra, cryptography, game theory, information security, mathematical modeling, etc.

Wei Jiang received the BS, MS, and PhD degrees from the Harbin Institute of Technology (HIT), China in 2004, 2006, and 2010, respectively. He is now an associate professor of Chinese Academy of Cyberspace Studies, Beijing, China. His research interests include network and information security, as well as social computing.

Xiaohui Liu received the MS degree from Dalian Maritime University in 2007. She is a lecturer at Beijing Information Technology College. She research interests include cryptography, network security, etc.

Hui Lu received the BEng degree in electronic science and technology from Southwest Jiaotong University, Chengdu, China, the MS degree in optical engineering from Southwest Jiaotong University, Chengdu, China, and the PhD degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications, Beijing, China

in 2003, 2006, and 2010, respectively. He is now an associate professor at the Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China. He was a research associate at the Institute of Microelectronics, Chinese Academy of Sciences from 2010 to 2017. In 2017, he joined Guangzhou University. His research interests include cyberspace security and intelligent attack-defence.



Zhihong Tian received the BS, MS, and PhD degrees from the Harbin Institute of Technology (HIT), China in 2001, 2003, and 2006, respectively. He is a professor, PhD supervisor, and dean of Cyberspace Institute of Advanced Technology, Guangzhou University. He is the standing director of CyberSecurity Association of China and the member of China Computer Federation. From 2003 to 2016, he worked at Harbin Institute of Technology. His current research interests include computer network and network security

Xiaojiang Du received the BS and MS degrees in electrical engineering from Automation Department, Tsinghua University in 1996 and 1998, respectively. He received the MS and PhD degrees in electrical engineering from the University of Maryland, USA in 2002 and 2003, respectively. He is a tenured full professor and the director of the Security And Networking (SAN) Lab in the Department of Computer and Information Sciences at Temple University, Philadelphia, USA. His research interests include security, wireless networks, and systems. He has authored over 400 journal and conference papers in these areas, as well as a book published by Springer. He has been awarded more than 6 million US Dollars research grants from the US National Science Foundation (NSF), Army Research Office, Air Force Research Lab, NASA, the State of Pennsylvania, and Amazon. He won the best paper award at IEEE GLOBECOM 2014 and the best poster runner-up award at the ACM MobiHoc 2014. He serves on the editorial boards of two international journals. He served as the lead chair of the Communication and Information Security Symposium of the IEEE International Communication Conference (ICC) 2015, and a co-chair of Mobile and Wireless Networks Track of IEEE Wireless Communications and Networking Conference (WCNC) 2015. He is (was) a Technical Program Committee (TPC) member of several premier ACM/IEEE conferences, such as INFOCOM (2007–2020), IM, NOMS, ICC, GLOBECOM, WCNC, BroadNet, and IPCCC. He is an IEEE fellow and a life member of ACM.