Hindawi
Complexity
Volume 2021, Article ID 6614941, 7 pages
https://doi.org/10.1155/2021/6614941

Review Article

Game-Based Trust in Complex Networks: Past, Present, and Future

Li Yi,[1,2] **Weidong Fang**,[1,2] **Wuxiong Zhang**,[1,2] **Weiwei Gao**,[1,2] **and Baoqing Li**[1,2]

[1]*Science and Technology on Micro-System Laboratory, Shanghai Institute of Micro-System and Information Technology, Chinese Academy of Sciences, Shanghai 201800, China*
[2]*University of Chinese Academy of Sciences, Beijing 100049, China*

Correspondence should be addressed to Weidong Fang; weidong.fang@mail.sim.ac.cn

Received 2 December 2020; Revised 4 February 2021; Accepted 9 February 2021; Published 27 February 2021

Academic Editor: Jianxin Li

As an efficient approach, the trust policy is implemented to defend against insider attacks in complex networks. However, the imperfection of trust relationships directly hinders the effort to quantitatively calculate trust value, especially in choosing a cooperative partner. Fortunately, the game theory is gradually concerned with addressing the above issue to further enhance security. In this paper, the game theory and the trust policy are reviewed briefly. Then, the research roadmap on game-based trust in complex networks is discussed and analysed deeply. Furthermore, some research directions in the near future are given. It is worth mentioning that our contributions not only describe the evolution of the game-based trust clearly but also suggest the trust mechanism based on the bounded rational game more suitable to uncertain information.

1. Introduction

With the rapid development of complex networks, many communication nodes are deployed to provide us a more convenient life. However, those increasing communication nodes without any trust policy are risky. Essentially, the trust policy in complex networks is used to confirm trust relationships between entities, while it faces the challenge of ever-growing complexity and uncertainty. How to maintain mutual trust and security in complex networks is becoming a growing concern.

From the perspective of information security, trust can be divided into two categories, namely, trust in human agents and trust in systems [1]. The characteristics of trusted human agents include honest and straight. You are honest if you keep your word and dishonest if you do not. You are straight if you follow the rules and crooked if you do not. The concept of trust in human agents is always opposed to malicious behaviours. By contrast, systems do not earn trust through behaviours, but rather their capabilities to resist any attempt of malicious manipulations. At this point, trusted systems are called secure. However, due to the development of artificial intelligence, many systems have obtained a sort of autonomy that suits their interest well, different from classical systems and meanwhile different from human agents. In fact, the intellectualization of devices leads to more unpredictability. In order to adapt to this tendency, combining trust policy with game theory is a viable idea.

Game theory provides a rich set of mathematical methods and models for exploring multilayer strategic decision-making, which has been widely applied in the field of network security. In the framework of classical game theory, it is always assumed that all game participants are absolutely rational, which has a great deviation from the actual situation. And people would indeed punish inappropriate behaviour, even if the behaviour conforms to selfish rationality [2]. Research groups tried to overcome this problem by establishing bounded rationality [3–5]. For example, evolutionary game theory has two characteristics: bounded rationality and repetitive games, which bring new ideas to deal with uncertain information [6].

The main contributions of this paper can be summarized as follows:

(i) Trust policies are categorized into three types: trust evaluation, zero trust, and full trust. And then we propose a hybrid scheme to satisfy requirements for different levels of security.

(ii) Trust mechanism based on the bounded rational game may be more suitable to ever-increasing uncertain information.

The purpose of this paper is to summarize the research progress of game-based trust and discuss the feasible future direction. The rest of this paper is organized as follows: in Section 2, we introduce the development of the game theory with absolute rationality and bounded rationality. We briefly overview three kinds of trust policies in Section 3. In Section 4, the game-based trust mechanisms are classified and discussed according to the application scenario. In Section 5, we look into the future research development direction of game-based trust. Finally, conclusions are provided in Section 6.

2. Game Theory

Game theory, a science that models and evaluates the behaviour of decision-making systems, has attracted extensive attention due to its application in economics more than half a century ago. The classical game theory can be divided into complete information game and incomplete information game according to the completeness of game information. On the other hand, it can be divided into the static game and dynamic game depending on whether there is a sequential order between actions. The above types were raised with the precondition of absolute rationality. Research groups found the limitations of this prerequisite due to the bounded rationality of decision-makers. Some methods are used to overcome the problem, such as reward and punishment mechanism, the fuzzy theory, and evolutionary game theory [7, 8]. Furthermore, game theory with bounded rationality can be applied not only to economics but also to network security. This section will give an overview of the study of game theory and security cooperation problems solved by game theory.

2.1. Classical Game Theory. Classical game theory initially took shape in the 1920s. In 1928, Von Neumann presented the minimax theorem to handle the most basic game with two persons in his paper about the social game. Then, in 1950, John Nash proposed the concept of Nash equilibrium [9], which was used to solve the problems of decision convergence in multiperson noncooperative games. Moreover, he proved the existence of Nash equilibrium and found out the solvability conditions in his doctoral thesis [10]. The minimax theorem and Nash equilibrium lay the foundation for the subsequent development of game theory. In the 1960s, John et al. used Bayesian prediction to consider the situation of incomplete information games [11]. In the 1980s, the dynamic game theory had been well developed and was applied to economics, resource allocation, and other fields [12, 13]. Since then, the classical game theory had come to a near standstill but had been applied more broadly. Recently there are still many scholars using game theory to solve the problem of resource allocation and trusted communication in complex systems [14–19].

2.2. Game Theory with Bounded Rationality. The game theory with bounded rationality mainly includes the following aspects: reward and punishment mechanism, Dempster–Shafer (D–S) theory, fuzzy theory, and evolutionary game. This part will respectively introduce these methods. In reward and punishment mechanisms, or contract theory, participants receive appropriately designed rewards or punishments based on their performance in order to encourage better cooperation. The D–S theory, also known as evidence theory, is a popular mathematical framework for dealing with uncertain information. As an inference theory in an uncertain environment, the D–S theory has the advantage of directly expressing "uncertainty" by assigning probabilities to a subset of a set consisting of multiple objects rather than to each individual object. There have been many scholars in actively exploring the combination of evidence theory and game theory [20–23]. On the other hand, fuzzy set theories, such as Pythagoras fuzzy set and shadow set, were also used to deal with the uncertain information in the game [8, 24]. As for evolutionary game theory, it combines the classical game theory and viewpoints of evolutionism. The research objects of the evolutionary game are often participant group, rather than the individual participants in classical game theory. Evolutionary game theory investigates the dynamic equilibrium problem in the evolution trend of group behaviours from the viewpoint of system theory. It can better adapt to the characteristics of the dynamic topology of network structure with a large number of participants in complex systems. The above methods are not mutually exclusive. Sometimes they are used in the meantime. For example, the reward and punishment mechanism could be regarded as the screening approach of the evolutionary game [7, 25].

2.3. Security Cooperation with Game Theory. The game exists widely in complex networks. Appropriate profit allocation schemes in conformity with selfish and collective rationality fall in the core of the cooperative game. So, cooperative schemes based on game theory are less likely to be violated. The game theory makes cooperation more secure. Recently, Zheng et al. put forward cooperative game-theoretic mechanisms to coordinate the three-echelon closed-loop supply chain with a fairness-minded retailer [16]. Furthermore, Wei et al. established an imperfect information Stackelberg game model [26]. It motivates service providers to select the optimal bidding strategy according to the overall utility. These research findings help to foster cooperation and achieve an equitable allocation of surplus profit. The stability and security of cooperation, therefore, are improved. However, there is often information asymmetry between decision-makers. At this point, decision-makers can overcome this information asymmetry by resorting to game theory based on reward and punishment mechanisms. Because of this nature of reward and punishment mechanisms, it is conceivable that there is great potential for using contract theory in complex networks to ensure cooperation and help design incentives [27]. For crowdsensing in the uncertain wireless scenario, Cao et al.

designed a game-theoretic approach based on an incentive mechanism to encourage the "best" neighbour mobile devices to share their own resource for sensing [28]. More cooperation reinforces the robustness and security of the system. As for evolutionary game theory, Liu et al. explored the use of evolutionary game theory to describe the long-term dynamic process of multiplayer game playing in coal-mine safety regulation under the condition of bounded rationality [25]. It provided a more effective solution to the study of complex multiplayer game problems. Although the security of systems is increased depending on game theory, there is no defence against malicious attack and undetected accidental failure. To cope with the demand for security, trust mechanisms are necessary.

3. Trust Policy

The concept of trust has been part of human history since antiquity. It is highly subjective and complex. In the meantime, trust has abundant interesting and important connotations. With the development of computer science and the Internet, various malicious attacks are emerging in an endless stream. People have come to realize the significance of trust in networks, especially in complex networks. Nowadays, the major trust policies could be divided into three categories: trust evaluation, zero trust, and full trust. The following part of this section will, respectively, discuss these three categories and propose a method to blend them.

3.1. Trust Evaluation. According to the historical behaviours and performance of human agents or systems, we can evaluate the trust degree of entities via the quantitative method. On the opposite side of malicious behaviours, the concept of trust in networks is often associated with reputation. Reputation, as a reference for the entity trust level, is based on historical events and the evaluation from other peers. Early research on information security focused on how to store and spread trust. Afterwards, they gradually evolved into research on trust itself and trust model [1]. The typical trust management paradigm in complex networks involves the collection of trust value, the storage of trust value and reputation, the aging of trust value, the weight of indirect information, the transfer of trust, and reputation. By synthesizing the above factors, we can obtain the trust value as follows:

$$T_{ij} = F\left(v_{ij}, iv_{ij}\right), \tag{1}$$

$$v_{ij} = G\left(h_{ij}, \lambda, r_j\right). \tag{2}$$

In equation (1), v_{ij} denotes entity i's direct trust value for entity j and iv_{ij} denotes entity i's indirect trust value for entity j. In equation (2), h_{ij} denotes the observation history of entity j, λ denotes the aging factor of historic observations, and r_j denotes the reputation of entity j.

Many scholars have made contributions to trust evaluation models and trust management schemes [29–31]. A complex trust evaluation model is proposed for the design of data aggregation in mobile sensor networks [32]. In this model, due to the dynamic topology of the network, each node maintains the trust score estimation list of its neighbour nodes based on beacon data collected in the neighbour nodes. Once the estimated trust score of one of its neighbours drops below the threshold, it is classified as a "damaged or failed" node. And then all the retweet data passing by the failed node is discarded or filtered. As for trust management, Fang proposed a time-window-based resilient trust management scheme in order to defend against the reputation time-varying attacks in wireless sensor network [33]. This scheme aims to distinguish malicious attackers with the compromised nodes. It needs a period of time to observe and analyse the behaviours of compromised nodes and then utilizes the difference judgment and the trend analysis to identify the abnormality of nodes' reputation value. Meanwhile, the control factor and the time window are introduced to verify and remove the compromised nodes from the suspected nodes. On the other hand, there are some schemes providing removed nodes with ways to be reinstated. For example, Li et al. proposed a multifactor reputation management scheme, which describes the initialization, update, storage, and punishment of trust values and the redemption for malicious nodes [34]. The scheme is based on the sensing behaviour, packet forwarding, and data fusion of sensor nodes. Furthermore, consensus techniques based on subjective logic are introduced to the trust management system. Ren proposed a trust management approach to provide trust data storage and trust generation for unattended wireless sensor networks [35]. For the former, a geographic hash table is deployed to identify storage nodes and reduce storage costs. For the latter, consensus techniques based on subjective logic are used to mitigate trust fluctuations caused by environmental factors.

3.2. Zero Trust and Full Trust. Zero trust is the situation that there is complete mistrust on at least one side. Authentication must be verified exactly for each collaboration. The contrary is full trust, where users trust the system completely because it is robust and cannot be manipulated by anyone.

In recent years, there have emerged concepts of the full trust, represented by blockchain [36], and the zero trust, represented by identity recognition [37], except for the above trust evaluation schemes. The blockchain is a decentralized database, which relies on the automatic operation of the program. Theoretically, it has proved that it is possible to change the data only by controlling more than half of the nodes. It has extremely high credibility, and the security threat only comes from the vulnerability of the program. On the other hand, due to the recent development of deep neural networks, the accuracy of identity recognition has been significantly improved. For systems that do not trust users at all, identity recognition can be required for each operation, which leads to the concept of zero trust.

3.3. Hybrid Scheme. The concepts of zero trust and full trust are not mutually exclusive. For example, Andrade combined blockchain with identity recognition, which uses the trusted blockchain system to verify suspected users [38]. Obviously, the resource costs of full trust, trust evaluation, and zero trust increase in turn, which are suitable for scenarios with different demands on the security level.

In order to break down this barrier and gain security with low resource cost, considering a clever combination mode of the three is a viable idea (see Figure 1). At first, the model determines the required security level according to node behaviours. For example, there needs to be a high level of security if the behaviour is initiating the account transfer and low level of security if just data transmission is requested. Then, identity recognition, known as zero trust, is implemented when high-level security is required and trust evaluation model is put into use in unmarked cases. In Figure 1, historical observations represent the historical cooperation between two entities. Distinguished from current observations or the latest record of collaboration, its influence is reduced via the aging factor. Considering the current and historical observations together, we can calculate the direct trust value. Moreover, blockchain, known as full trust, is used to transmit information of indirect observations.

However, the process from the direct and indirect trust to the final decision is not clear. Many solutions have been raised for the decision-making process, among which the game theory achieves good effectiveness.

4. Game-Based Trust

In order to improve the robustness and security of networks, the concepts of game-based trust have been introduced into various types of networks. There are two main paradigms at the junction of trust mechanism and game theory (see Figure 2). One uses game theory to synthesize direct trust and indirect trust for decision-making. In the other paradigm, game theory based on indirect information is applied in calculating indirect trust value.

According to the degree of interaction with human entities in networks, application scenarios are roughly divided into three categories: pure systems, social-aware mechanisms, and those that need to interact with users. The rest of this section will respectively discuss these three categories.

4.1. Pure System. The pure system application scenario refers to the system running automatically with almost no interaction with human users. On this occasion, trust is only the trust between devices. The pure system performance index is mainly the efficiency and security [39, 40]. For example, a new trust-Stackelberg game model was proposed in dynamic cognitive radio networks [41]. The authors designed an adaptive trust evolutionary learning algorithm based on evolutionary game theory to achieve the game equilibrium, aimed at improving energy efficiency and defending against insider attacks in cooperative cognitive radio networks.

4.2. Social-Aware. A social-aware system is one in which the user's social information is collected as a parameter to evaluate trust during the decision-making process. There are usually higher levels of trust and trustworthiness between friends and people with more cooperation, both because we believe our friend is more trustworthy and because social interaction enhances higher levels of cooperation between those who interact repeatedly over time [42, 43]. Therefore, participants' social relationships can provide a good reference for game-based trust. For participants, the bounded rational trust game not only strengthens the cooperation with other nodes but also reduces the probability of being deceived due to subjective feelings and information asymmetry. In such scenarios, besides utility and security, users' privacy protection should also be considered in terms of performance indicators. The "likes" and comments in online social networks can be used to reflect social relations, and then initial trust values can be assigned in the bootup mechanism. This method only uses publicly available information, so as to reduce the risk of privacy leakage [44]. In addition, as devices become more and more intelligent, it is also a key concept to define expected credibility by considering the social consciousness of the device itself [45].

4.3. User Interaction. An application scenario that requires interaction with users refers to a system that often interacts with people, sometimes involved in the decision-making process. In this type of scenario, performance is about not only utility and security but also whether it facilitates user cooperation [46]. For example, a new trust management mechanism based on evolutionary game theory was proposed in self-organizing complex networks, with a corresponding node punishment mechanism to enhance cooperative behaviours [47]. In cognitive radio networks, Bennaceur et al. proposed another trust game model to take into consideration the penalty of the malicious users. By introducing the trust game model of cooperative sensing spectrum, the secondary users are encouraged to choose the honest strategy by sending correct sensing outcomes [48].

For the different requirements of the three types of application scenarios, the trust mechanisms based on the bounded rational game theory can achieve better performance and adapt itself to the trend of devices intellectualization, which is a direction worthy of research.

5. Future Directions of Game-Based Trust

When the concept of trust is applied to network systems, the selfish and rational aspect of trust is mainly considered. Entities with rationality expect to cooperate with other trusted entities. But the purpose of confirming trusted entities may or may not be achieved under the impact of information incompleteness. In order to better accomplish this goal, the research groups have put forward a scheme combining game theory and trust. The trust policies based on classical game theory perform well under the scenario with relatively fixed mode. But under various complex application scenarios with uncertain characteristics, the game-based trust mechanisms with bounded rationality can improve the utility and security of the system.

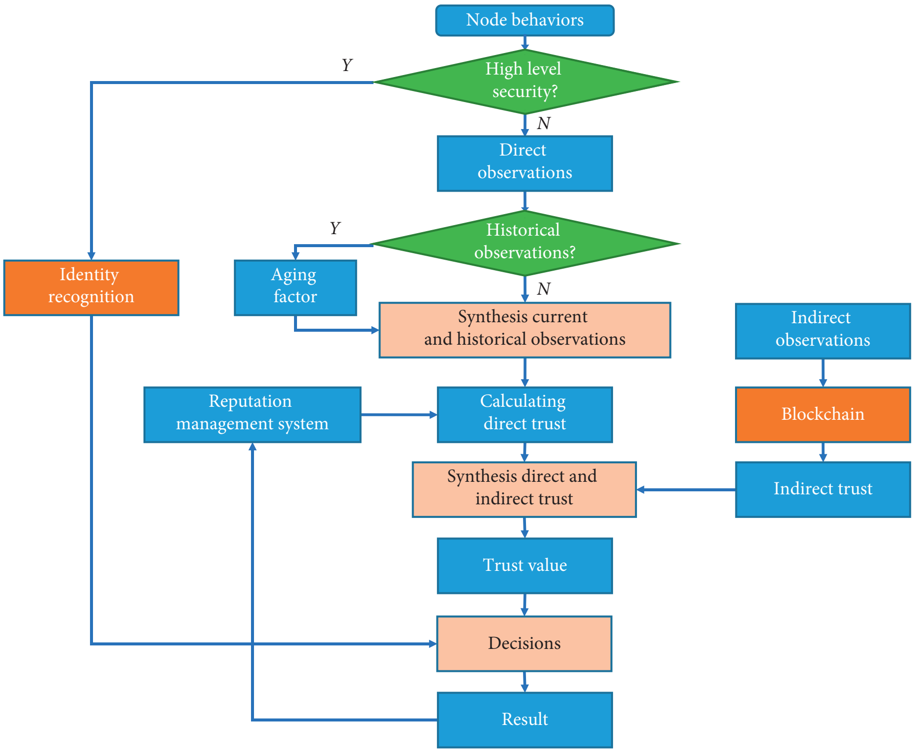

Figure 1: A hybrid scheme: identity recognition is used to satisfy requirements of high-level security, and blockchain is used to transmit indirect information.

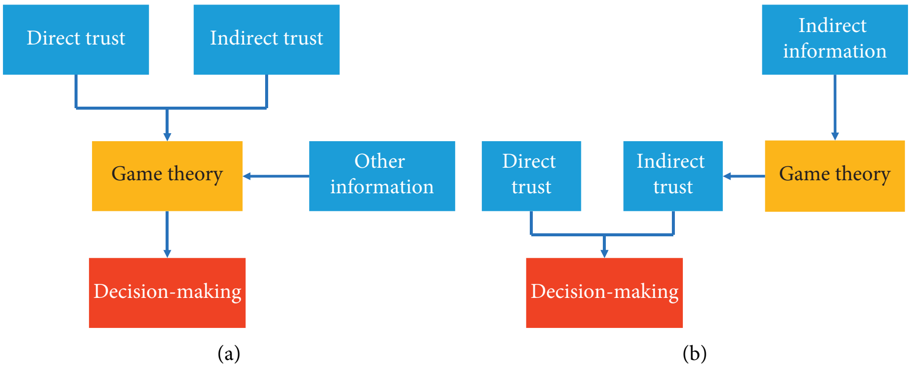

Figure 2: Game-based trust. (a) Game theory is used to synthesize direct trust and indirect trust. (b) Acquiring indirect trust value by using game theory.

In view of the development of artificial intelligence, more intelligent device nodes are bound to appear in the future, bringing more uncertainty. We suggest that the trust mechanisms based on bounded rational game theory can better adapt to such scenarios and deal with possible security risks. At present, the research on game-based trust with bounded rationality is not enough, which is a direction worthy of development.

However, bounded rationalization will bring more energy costs. So, how to save cost is an important problem. Under different scenarios and different levels of security requirements, it is a feasible idea to reasonably combine the concepts of zero trust and full trust with the trust evaluation policies based on bounded rational game theory. For example, the blockchain technology can be used to disseminate the indirect trust information in the trust evaluation mechanism. This method improves the propagation mode of indirect trust information and could save the communication cost of game-based trust mechanisms with bounded rationality.

6. Conclusions

In this paper, we have reviewed game theory with absolute rationality or bounded rationality and catalogized three trust policies. On this basis, the game-based trust policies are classified and discussed according to the application scenario with pure systems, social-aware mechanisms, and user interaction mechanisms. Through the analysis of existing literature, we believe that the game theory of bounded rationality has a good performance in dealing with uncertain information and can be combined with a trust mechanism to better evaluate trust. There are two main contributions in this paper: (1) there are three trust policies: trust evaluation, zero trust, and full trust. And then a hybrid scheme to satisfy requirements for different levels of security is proposed. (2) It is suggested that trust mechanisms are based on the bounded rational game more suitable to ever-increasing uncertain information.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (nos. 51874300 and 61471346), Shanghai Municipal Natural Science Foundation (no. 18ZR1437600), Shanghai Municipal Key Project (no. 19511132401), and the National Key Research and Development Program of China-Internet of Things and Smart City Key Program (nos. 2019YFB2101600, 2019YFB2101602, and 2019YFB2101602-03).

References

[1] A. Jøsang, “The right type of trust for distributed systems,” in *Proceedings of the 1996 Workshop on New Security Paradigms*, pp. 119–131, New York, NY, USA, September 1996.

[2] J. Berg, J. Dickhaut, and K. McCabe, “Trust, reciprocity, and social history,” *Games and Economic Behavior*, vol. 10, no. 1, pp. 122–142, 1995.

[3] A. Rubinstein, *Modeling Bounded Rationality*, MIT press, Cambridge, MA, USA, 1998.

[4] J. Geanakoplos, D. Pearce, and E. Stacchetti, “Psychological games and sequential rationality,” *Games and Economic Behavior*, vol. 1, no. 1, pp. 60–79, 1989.

[5] M. Rabin, “Incorporating fairness into game theory and economics,” *The American Economic Review*, vol. 83, no. 5, pp. 1281–1302, 1993.

[6] K. Komathy and P. Narayanasamy, “Secure data forwarding against denial of service attack using trust based evolutionary game,” in *Proceedings of the VTC Spring 2008-IEEE Vehicular Technology Conference*, pp. 31–35, Birmingham, EN, UK, May 2008.

[7] H. Xie, W. Wang, and X. Zhang, “Evolutionary game and simulation of management strategies of fallow cultivated land: a case study in Hunan province, China,” *Land Use Policy*, vol. 71, pp. 86–97, 2018.

[8] Y. Z. J. Yao, “Game theoretic approach to shadowed sets: a three-way tradeoff perspective,” *Information Sciences*, vol. 507, pp. 540–552, 2020.

[9] J. F. Nash, “Equilibrium points in n-person games,” *Proceedings of the National Academy of Sciences*, vol. 36, no. 1, pp. 48-49, 1950.

[10] J. Nash, “Non-cooperative games,” *The Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, 1951.

[11] J. C. Harsanyi, “Games with incomplete information played by “bayesian” players, I-iii Part I. The basic model,” *Management Science*, vol. 14, no. 3, pp. 159–182, 1967.

[12] J. F. Reinganum, “A dynamic game of R and D: patent protection and competitive behavior,” *Econometrica*, vol. 50, no. 3, pp. 671–688, 1982.

[13] M. Pohjola, “Applications of dynamic game theory to macroeconomics,” *Dynamic Games and Applications in Economics*, vol. 265, pp. 103–133, 1986.

[14] A. Paudel, K. Chaudhari, C. Long, and H. B. Gooi, “Peer-to-peer energy trading in a prosumer-based community microgrid: a game-theoretic model,” *IEEE Transactions on Industrial Electronics*, vol. 66, no. 8, pp. 6087–6097, 2018.

[15] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long, “Peer-to-Peer energy trading in a Microgrid,” *Applied Energy*, vol. 220, pp. 1–12, 2018.

[16] X.-X. Zheng, Z. Liu, K. W. Li, J. Huang, and J. Chen, “Cooperative game approaches to coordinating a three-echelon closed-loop supply chain with fairness concerns,” *International Journal of Production Economics*, vol. 212, pp. 92–110, 2019.

[17] S. Safarzadeh and M. Rasti-Barzoki, “A game theoretic approach for assessing residential energy-efficiency program considering rebound, consumer behavior, and government policies,” *Applied Energy*, vol. 233-234, pp. 44–61, 2019.

[18] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang, “Energy Demand Side Management within micro-grid networks enhanced by blockchain,” *Applied Energy*, vol. 228, pp. 1385–1398, 2018.

[19] F. Tang, Z. M. Fadlullah, N. Kato, F. Ono, and R. Miura, “AC-POCA: anticoordination game based partially overlapping channels assignment in combined UAV and d2d-based networks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1672–1683, 2018.

[20] X. Deng, W. Jiang, and Z. Wang, “Zero-sum polymatrix games with link uncertainty: a Dempster-Shafer theory solution,” *Applied Mathematics and Computation*, vol. 340, pp. 101–112, 2019.

[21] Y. Han and Y. Deng, “A novel matrix game with payoffs of Maxitive Belief Structure,” *International Journal of Intelligent Systems*, vol. 34, no. 4, pp. 690–706, 2019.

[22] X. Deng and W. Jiang, “D number theory based game-theoretic framework in adversarial decision making under a fuzzy environment,” *International Journal of Approximate Reasoning*, vol. 106, pp. 194–213, 2019.

[23] H.-G. Peng, X.-K. Wang, T.-L. Wang, and J.-Q. Wang, “Multi-criteria game model based on the pairwise comparisons of strategies with Z-numbers,” *Applied Soft Computing*, vol. 74, pp. 451–465, 2019.

[24] Y. Han, Y. Deng, Z. Cao, and C. T. Lin, “An interval-valued Pythagorean prioritized operator-based game theoretical framework with its applications in multicriteria group decision making,” *Neural Computing and Applications*, vol. 32, pp. 1–19, 2019.

[25] Q. Liu, X. Li, and X. Meng, “Effectiveness research on the multi-player evolutionary game of coal-mine safety regulation in China based on system dynamics,” *Safety Science*, vol. 111, pp. 224–233, 2019.

[26] W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, “Imperfect information dynamic Stackelberg game based resource allocation using hidden markov for cloud computing,” *IEEE Transactions on Services Computing*, vol. 11, no. 1, pp. 78–89, 2018.

[27] Y. Zhang, M. Pan, L. Song, Z. Dawy, and Z. Han, "A survey of contract theory-based incentive mechanism design in wireless networks," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 80–85, 2017.

[28] B. Cao, S. Xia, J. Han, and Y. Li, "A distributed game methodology for crowdsensing in uncertain wireless scenario," *IEEE Transactions on Mobile Computing*, vol. 19, no. 1, pp. 15–28, 2019.

[29] M. Alam, K. Kuga, and J. Tanimoto, "Three-strategy and four-strategy model of vaccination game introducing an intermediate protecting measure," *Applied Mathematics and Computation*, vol. 346, pp. 408–422, 2019.

[30] W. Fang, W. Zhang, W. Chen et al., "Trust-based Attack and Defense in Wireless Sensor Networks: A Survey," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 2643546, 20 pages, 2020.

[31] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collecting in smart city," *IEEE Transactions on Industrial Informatics*, vol. 99, p. 1, 2020.

[32] N. Meghanathan, "A distributed trust evaluation model for wireless mobile sensor networks," in *Proceedings of the 2014 11th International Conference on Information Technology*, pp. 186–191, Bitola, Macedonia, April 2014.

[33] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution," *Science China Information Sciences*, vol. 60, no. 4, Article ID 040305, 2017.

[34] F. Fang, J. Li, and J. Li, "A reputation management scheme based on multi-factor in WSNs," in *Proceedings of the 2013 International Conference On Mechatronic Sciences, Electric Engineering and Computer (Mec)*, pp. 3843–3848, Shenyang, China, December 2013.

[35] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1409–1423, 2013.

[36] X. Yang, G. Wang, H. He, J. Lu, and Y. Zhang, "Automated demand response framework in ELNs: decentralized scheduling and smart contract," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 58–72, 2019.

[37] S. P. Hsu, J. M. Ling, A. F. Messenger, and B. W. Evans, *Remote Identity Verification Technique Using a Personal Identification Device*, U.S. Patent, USA, Article ID 6182221, 2001.

[38] M. Andrade, *Systems and Methods for Providing Block Chain-Based Multifactor Personal Identity Verification*, U.S. Patent, USA, Article ID 9985964, 2018.

[39] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5971–5980, 2019.

[40] Y. Li, H. Xu, Q. Cao, Z. Li, and S. Shen, "Evolutionary game-based trust strategy adjustment among nodes in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 2, pp. 818903–818912, 2015.

[41] H. Fang, L. Xu, J. Li, and K.-K. R. Choo, "An adaptive trust-Stackelberg game model for security and energy efficiency in dynamic cognitive radio networks," *Computer Communications*, vol. 105, pp. 124–132, 2017.

[42] D. D. Cagno and E. Sciubba, "Trust, trustworthiness and social networks: playing a trust game when networks are formed in the lab," *Journal of Economic Behavior& Organization*, vol. 75, no. 2, pp. 156–167, 2010.

[43] S. Shen, L. Huang, E. Fan, K. Hu, J. Liu, and Q. Cao, "Trust dynamics in WSNs: an evolutionary game-theoretic approach," *Journal of Sensors*, vol. 2016, pp. 1–10, 2016.

[44] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Towards trustworthy multi-cloud services communities: a trust-based hedonic coalitional game," *IEEE Transactions on Services Computing*, vol. 11, no. 1, pp. 184–201, 2018.

[45] L. Militano, A. Orsino, G. Araniti, M. Nitti, L. Atzori, and A. Iera, "Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems," *Computer Networks*, vol. 111, pp. 141–151, 2016.

[46] X. Wang, Y. Wu, Y. Ren et al., "An evolutionary game-based trust cooperative stimulation model for large scale MANETs," *International Journal of Distributed Sensor Networks*, vol. 9, no. 6, Article ID 245017, 2013.

[47] H.-J. Li, Q. Wang, S. Liu, and J. Hu, "Exploring the trust management mechanism in self-organizing complex network based on game theory," *Physica A: Statistical Mechanics and Its Applications*, vol. 542, Article ID 123514, 2020.

[48] J. Bennaceur, H. Idoudi, and L. A. Saidane, "A trust game model for the cognitive radio networks," in *Proceedings of the 2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pp. 1–5, Paris, France, November 2016.