Secure and Reliable D2D Communications with Active Attackers: A Game-Theoretic Perspective and Machine Learning Approaches

Yijie Luo(✉), Yang Yang, Sixuan An, and Zhibin Feng

Army Engineering University of PLA, Nanjing, China
yijieluo@sina.com, sheep_l009@163.com,
ll02719288@qq.com, fengzbl995@163.com

Abstract. Frequent communications among massive terminal devices are ubiquitous in forthcoming 5G Internet of Thing (IoT) networks. It strengthens links of massive machine-type-communication (MMTC), pushes forward the process of Internet of everything. However, due to continual interactions among different devices and the broadcast characteristic of wireless channels, it also brings new security challenges. Recently, physical layer security launches a new solution to guarantee information theoretic security. To enhance the physical layer security performance of massive intelligent devices, especially in D2D communications, the game theory and machine learning methods are introduced. In this paper, we first review physical layer security problems on D2D communications under different attack scenarios. Game theory is proposed to describe hierarchical and heterogeneous interactions among legitimate users and active attackers in 5G IoT networks, then some distributed machine learning methods are proposed to obtain equilibrium states among different agents. Moreover, numerical results are provided to verify availability and efficiency of proposed game-theoretic learning approaches. Finally, we discuss open issues and future research directions in term of anti-eavesdropping and anti-jamming problems in D2D communications when facing active attackers.

Keywords: D2D communications · Full-duplex active eavesdropper · Physical layer security · Hierarchical game · Distributed machine learning

1 Introduction

The fifth generation (5G) mobile communication system is being quickly deployed at the present, and studies on key technologies of the next generation 5G and 6G networks are opening up. We can see that the future mobile communications focus on applications of artificial intelligence (AI) from the published literature, not simple superposition of them, but deep integration of huge application and intelligent networks [1–3]. AI [1, 2], edge computing [3] and Internet of Thing (IoT) technologies will drive important innovations of mobile communications, ever change the actual world in the future [4]. Frequent interactions among lots of devices will exist everywhere in the

M. Guan and Z. Na (Eds.): MLICOM 2020, LNICST 342, pp. 519–533, 2021.
https://doi.org/10.1007/978-3-030-66785-6_55

future, diverse communication requirements of different users face huge challenges, and AI technology, such as machine learning [5], will act an important part in it.

In the next 5G mobile communications or IoT networks, since communications between device to device (D2D) or machine to machine (M2M) will be frequent, it is difficult to guarantee communication security. Physical layer security will be a valid supplement and enhancement for communication network security. Adopting transmission technologies (artificial jamming [6], full-duplex receiving [7], multiple antenna [8] and relay cooperation [9]) to make transmission rates larger than eavesdropping rates, perfect physical layer security can be achieved. However, due to the existence of massive users and information asymmetric of different users, it is difficult to obtain perfect physical layer security. Moreover, when attackers become more active and intelligent, that is to say, they can launch different attacks flexibly, secure and reliable communications among a lot of devices in 5G IoT networks can be hardly ensured.

Game theory is a valid mathematic tool, which can analyze competition and cooperation among multi-users, it is suitable to model physical layer security and anti-jamming problem of legitimate users against active attacks. Furthermore, intelligent devices can achieve better communication performance through machine learning methods. Therefore, by way of combination of game theory and machine learning methods, not only joint physical layer security and anti-jamming problem can be solved in theory, but also robust anti-eavesdropping and anti-jamming strategies can be obtained in reality. At the present, game theory and machine learning methods have been extensively studied on resource management, power control in cellular networks and dynamic spectrum access in cognitive radio networks. Moreover, they have been already used under active eavesdropping and intelligent jamming scenarios [10–12].

D2D communication is the direct communication between cellular users without forward by the base station. In the underlay way, D2D users have the opportunity to share the same spectrum of cellular users to transmit messages directly between them. In the future 5G IoT networks, D2D communications will extensively exist. In D2D communications, on one hand, strategies-making of distributed D2D users is asynchronous. On the other hand, there exists a natural hierarchical structure between cellular users and D2D users. Therefore, it is very suitable to use hierarchical and heterogeneous game-theoretic learning methods to combat active attackers in D2D communications.

In the following sections, we first review security threats in D2D communications with different active attacks, then illustrate applications of the game theory and machine learning methods for physical layer security and anti-jamming in D2D communications, finally we propose the future research directions and open issues in D2D communications with active attacks from the game theory perspective.

2 Review of Anti-eavesdropping and Anti-jamming in D2D Communications

Physical layer security problems are always studied with the assumption that eavesdroppers are passive. That is to say, when they wiretap confidential messages of legitimate users, they always keep silent. Compared with passive eavesdroppers, active attackers will do much more harm to legitimate users. On one hand, active attackers can launch active jamming attack to destroy reliable communications among legitimate users. On the other hand, active attackers can switch different attack types due to different attack aims, and they can adaptively adjust their attack strategies to bring more destruction for legitimate users.

We can divide active attackers into active eavesdroppers and active jammers according to attack types of them. Due to the duplex mode, active eavesdroppers can be further divided into half-duplex active eavesdroppers and full-duplex active eavesdroppers. The former ones only launch eavesdropping or jamming at different time slots, while the last ones can use two attack modes simultaneously. Active jammers are also called smart jammers, who can intelligently adjust their jamming power or channels to destroy reliable communications among legitimate users. Figure 1, 2 and 3 illustrate the scenarios of secure and reliable D2D communications with different active attackers. We analyze technology challenges in D2D communications with these kinds of active attackers in this section.

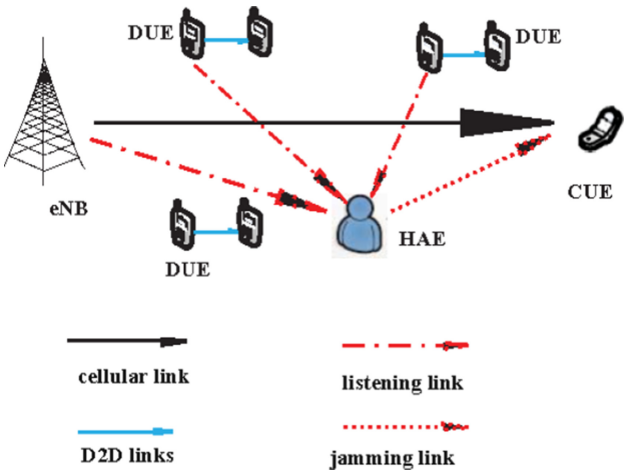

Fig. 1. Illustration of secure D2D communications with a half-duplex active eavesdropper.

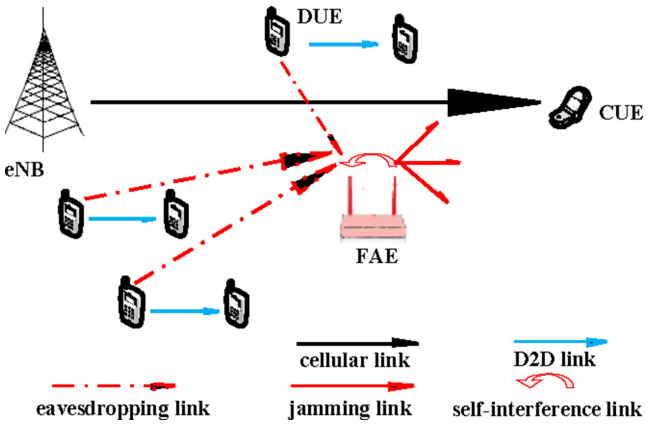

Fig. 2. Illustration of secure D2D communications with a full-duplex active eavesdropper.

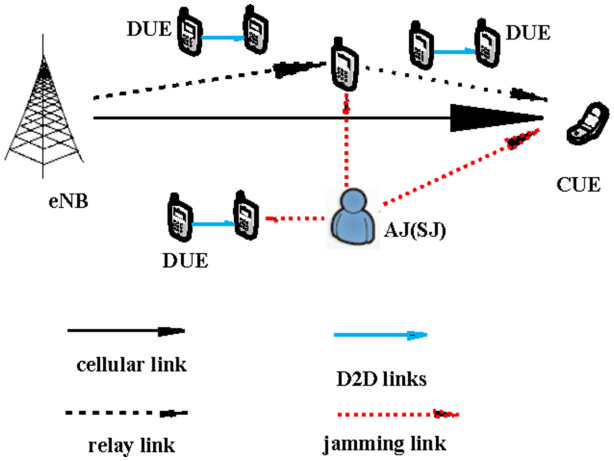

Fig. 3. Illustration of reliable D2D communications with an active jammer.

Half-Duplex Active Eavesdropper (HAE): Considering eavesdroppers become more intelligent and more selective, that is to say, they can select to passively eavesdrop private transmission among legitimate users, or actively jam them to destroy reliable communications, they are called half-duplex active eavesdroppers.

Full-Duplex Active Eavesdropper (FAE): If active eavesdroppers are of more hardware resources, they can launch eavesdropping and jamming attacks simultaneously, they are called full-duplex active eavesdroppers.

Active (Smart) Jammer (AJ/SJ): Active or smart jammers can adaptively adjust their jamming power or channels, and finally to decrease transmission rate and communication reliability of legitimate users.

If eavesdroppers can select passive eavesdropping or active jamming, legitimate users want to optimize their achievable secrecy rates or transmission rates accordingly. In [15], power allocation optimization was studied to improve the average achievable secrecy rate of legitimate users with a half-duplex active eavesdropper. When this kind of eavesdroppers intrude into D2D communications, not only the cooperation between cellular users and D2D users, but also the countermeasure between legitimate users and the half-duplex active eavesdropper should be joint considered. In [16], with the help of D2D cooperative relay and friendly jammers, the average achievable secrecy rate of the cellular user was enhanced with a half-duplex active eavesdropper.

Compared with the half-duplex active eavesdropper, it does much more harm to legitimate users when the active eavesdropper works on the full duplex mode. Firstly, the full-duplex active eavesdropper can carry out wiretapping and jamming attacks at the same time, anti-eavesdropping and anti-jamming demands of legitimate users should be jointly considered. Secondly, not only the inner interference between cellular users and D2D users should be considered, but also the outer jamming brought by the full-duplex eavesdropper should be referred to. In [10], transmission power of legitimate users or jamming power of the full-duplex active eavesdropper was hierarchically optimized to combat each other. The active eavesdropper was regarded as a jamming-aided eavesdropper in this works, where jamming attacks were launched to facilitate the eavesdropping, and the goal was to maximize the wiretap rate. While in [17], transmission rate of the cellular user and achievable secrecy rate of D2D users were joint optimized, while the full-duplex active eavesdropper carried out eavesdropping and jamming attacks at the same time to pursue the completely opposite goal.

Smart jammers can adaptively modify jamming channel strategy or jamming power to maximize jamming effects on legitimate users. Some researches considering that under smart jamming scheme, how to combat smart jammers through channel allocation and power control [18–24]. In [23], based on the spectrum waterfall, a recursive convolutional neural network was designed and a deep learning algorithm was proposed to combat dynamic and intelligent jammers. In [24], to combat a smart jammer, power control of the transmitter and relay were jointly optimized. In D2D communications, when smart jammers intrude, the inner interference should be avoided as soon as possible, and the outer jamming should be reduced to maintain robust transmission.

3 Game-Theoretic Learning Methods for Secure and Reliable D2D Communications

In the above section, we have analyzed new challenges for maintaining secure and reliable D2D communications when facing with active attackers. Then in this section, we study how multiple intelligent devices to enhance their anti-eavesdropping and anti-jamming performance by means of mutual cooperation and self-learning with game-theoretic learning methods. On one hand, in the future mobile communication networks or IoT networks, different intelligent devices are of different priorities, and their spectrum access or power control decisions are made asynchronously, so it is appropriate to use game theory to model complex interactions among them. On the other hand, not only the information exists in different distributed D2D (M2M) users, but

also the one between legitimate users and vicious attackers are asymmetrical. Moreover, they don't want to interact with their information, machine-learning based methods can be applied to improve physical layer security and anti-jamming performance in D2D communications.

Now we discuss how to apply game theory and machine learning methods under different active attack scenarios in D2D communications.

3.1 Game-Theoretic Learning Methods Against Half-Duplex Active Eavesdroppers

When eavesdroppers become active and intelligent, it means that they can select different attack types, passive eavesdropping or active jamming. If they work on the half-duplex mode, they can switch between the two attack types. Therefore, the cooperation among legitimate users and the confrontation between legitimate users and half-duplex active eavesdroppers can be formulated as a non-cooperative game or hierarchical game. In [15], the scenario was considered that the transmitter can allocate power to transmit data and broadcasting artificial interference, while the active eavesdropper can select to work as a passive eavesdropper or an active jammer under the half-duplex constraint. The strategic and extensive wiretap games were proposed and the pure-strategy and mix-strategy equilibrium were proved.

In D2D communications, when half-duplex active eavesdroppers intrude, cooperative relay or friendly jammer selection of D2D users and attack type selection of active eavesdroppers can be studied under the game framework. In [28], the cooperative D2D node selection problem of the base station and the attack type selection problem of the active eavesdropper were jointly modeled as a non-cooperative game. A learning algorithm based on fictitious-play was proposed and the mixed-strategy Nash equilibrium of the proposed game was reached. In [16], a Stackelberg game was proposed to formulate the competition between legitimate users and active eavesdropper, and a Q-learning based algorithm was proposed to obtain the mixed-strategy Stackelberg equilibrium.

In the above researches, we can find that as attackers becoming more and more intelligent. To combat them, some machine learning approaches were gradually employed to solve the physical layer security and anti-jamming problem. Not only legitimate users, but also active eavesdroppers have learning abilities to a certain degree. When active eavesdroppers can work on the full duplex mode, and can adaptively modify their jamming power, some more complex learning algorithms should be proposed to update power or spectrum strategies of legitimate users against them.

3.2 Game-Theoretic Learning Methods Against Full-Duplex Active Eavesdroppers

In general wireless networks, some game models have been utilized to model the confrontation between legitimate uses and full-duplex active eavesdroppers. In [10, 29], the power decision processes between legitimate users and the full-duplex active eavesdropper were studied at a Stackelberg game framework, the existence of the

Stackelberg equilibrium was proved, and heuristic legitimate power and jamming power allocation algorithms were proposed. In [30], the jamming power optimization of the full-duplex active eavesdropper and the transmission power optimization of the legitimate transmitter were formulated as a non-cooperative game, the sufficient conditions for the existence of the pure-strategy Nash equilibrium was derived, and the mixed-strategy Nash equilibrium was obtained by a fictitious-play based algorithm. Furthermore, in consideration of the cooperation among legitimate users and the confrontation between legitimate users and active eavesdroppers in a uniform framework, [31] proposed a three-stage Stackelberg game scheme among the transmitter, multiple relays and the full-duplex active eavesdropper, achieved cooperative communication, decreased the wiretapping probability and improved the secrecy performance.

We introduced the full-duplex active eavesdroppers into D2D communications. In [18], we formulated sequential power strategies of the base station, multiple D2D users and the full-duplex active eavesdropper to be a multi-layer Stackelberg game. Moreover, we proposed a hierarchical power control algorithm joint based on best response (BR) and stochastic learning automata (SLA) to enhance achievable secrecy rates of all D2D users and the transmission rate of the cellular user. And furthermore, in [32], we joint considered D2D relay selection, power control of the cellular user, and jamming power optimization of the active eavesdropper in a three-tier Stackelberg game, and a hierarchical and heterogeneous algorithm based on SLA and Q-learning was proposed to achieve the mixed-strategy Stackelberg equilibrium.

From the researches above, we can find hierarchical game have been applied to study the joint anti-jamming and physical layer security problem when facing with full-duplex active eavesdroppers. Moreover, we combine multi-tier hierarchical game and distributed machine learning methods to analyze and study the complex interactions among cellular users, D2D users and full-duplex active eavesdroppers.

3.3 Game-Theoretic Learning Methods Against Smart Jammers

When facing with smart jammers, hierarchical game can be also applied to describe dynamic interactions between legitimate users and smart jammers. Some researches considering that under smart jamming scheme, how to combat smart jammers through power control and channel allocation. Authors in [18] formulated the anti-jamming problem as a Stackelberg game, in which legitimate user was regarded as the leader, smart jammer as the follower, both changed their power strategies to maximize their utility. In [33], a Bayesian Stackelberg game was proposed to model anti-jamming scheme with the uncertainty of channel state and transmission cost. In [34], authors proposed an anti-jamming Stackelberg game in wireless networks, in which relay nodes were introduced and worked as the vice leader in the proposed game. And in [35], the discrete power control problem on anti-jamming was modeled as a Stackelberg game, and a hierarchical learning algorithm was proposed.

In [36], we formulated the hierarchical competitive relationship between a user and jammer as a Stackelberg game, and proposed a hybrid learning algorithm based on Q-learning and multi-armed bandit (MAB) for combating smart jamming. In D2D communications, when smart jammers intrude, the inner interference should be avoided

as soon as possible, and the outer jamming should be reduced to maintain robust transmission. Therefore, not only the competition and cooperation between cellular users and D2D users should be considered, but also the dynamic confrontation between legitimate users and smart jammers should be studied.

4 Numerical Results and Discussions

In this section, we will provide some numerical results with different active attackers and demonstrate the availability and efficiency of hierarchical game learning methods proposed in the former section.

4.1 Half-Duplex Active Eavesdropping Scenario

Under the system model in Fig. 1, we set up a cellular cell, where an evolved Node B (eNB) located on the center of a square area of 1 km * 1 km, and a cellular user and N D2D users are randomly located on the square area of 0.5 km * 0.5 km centered by the eNB, while the active eavesdropper is randomly located between the square area of 0.5 km * 0.5 km and 1 km * 1 km around the eNB. For our simulations, suppose that the transmit power of the eNB, all D2D users and the half-duplex active eavesdropper are 1 W, 0.1 W, and 0.1 W respectively. Considering that the half-duplex active eavesdropper can select passive eavesdropping or active jamming attack pattern, legitimate users cooperative with each other to combat it.

Firstly, considering that the hierarchical structure between the cellular user and all D2D users, we formulate their hierarchical interactions as a Stackelberg game to combat the half-duplex active eavesdropper. Furthermore, the cooperative power control problem among all D2D users is modeled as an exact potential game and a learning algorithm based on SLA is proposed to converge to the mixed-strategy Nash equilibrium of the lower-tier game, finally the Stackelberg equilibrium is received. The performance comparison of the proposed algorithm with selfish D2D power control algorithm (SDPCA) and the random selection algorithm (RSA) is presented in Fig. 4. We can see that the sum utility, which describes the tradeoff between secure requirements and power costs of all D2D users, decreases with the active jamming probability of the active eavesdropper, and the proposed algorithm outperforms other two algorithms.

Secondly, in consideration of the adaptive strategy selection of the half-duplex active eavesdropper, joint relay selection and friendly jamming power control of legitimate users and attack pattern selection of the active eavesdropper is formulated as a non-cooperative game. In the proposed game, a "best" D2D user is chosen to relay the confidential message of the cellular user, and other $N - 1$ D2D users working as friendly jammers to improve the average secrecy rate of the cellular user together. Then we propose a fictitious-play based algorithm to obtain the mixed-strategy Nash equilibrium of the proposed game. Figure 5 shows the performance advantage of the proposed algorithm compared with the nearest neighbor relay selecting algorithm with the increasing number of D2D users.

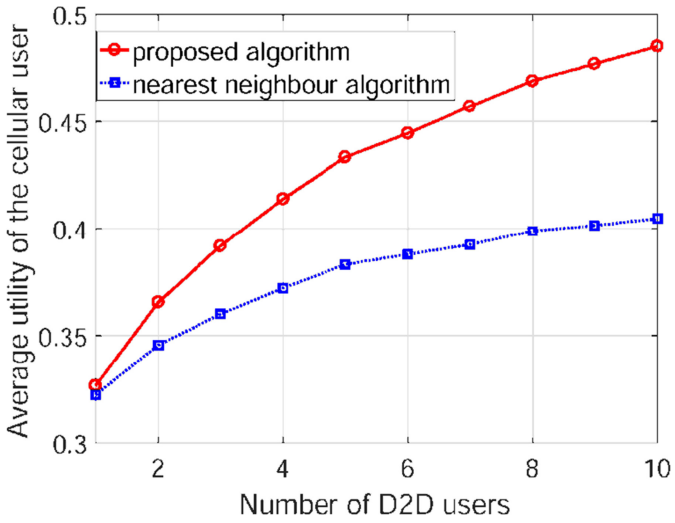

Fig. 4. Utility of the cellular user versus number of D2D users with a half-duplex active eavesdropper

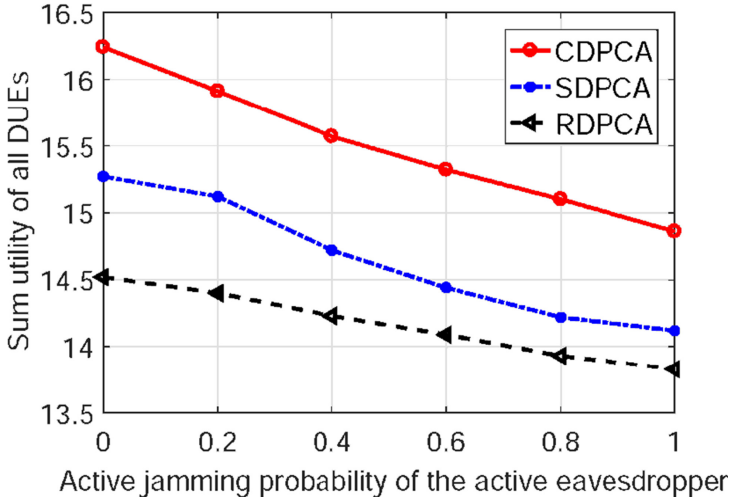

Fig. 5. Utility of all D2D users versus jamming probability of a half-duplex active eavesdropper

4.2 Full-Duplex Active Eavesdropping Scenario

The simulation under the full-duplex active eavesdropping scenario is made under the system model in Fig. 2. We first let the eNB on the origin of coordinates, the coordinates of the cellular user is (200 m, 200 m), 5 D2D users are randomly located in the square area of 300 m, 300 m, and the full-duplex active eavesdropper is located at 500 m, 500 m. Suppose that transmission power sets of the cellular user and the full-

duplex active eavesdropper are $\mathcal{P}_C = \mathcal{P}_A = \{0.2, 0.4, 0.6, 0.8, 1\}$ W, and the transmission power set $\mathcal{P}_D = \{0.02, 0.04, 0.06, 0.08, 0.1\}$ W is shared by all D2D users. In this situation, we consider that the full-duplex active eavesdropper can modify its jamming power to destroy the secure transmission of the cellular link and the reliable communication of D2D links, while the cellular user and all D2D users can select their suitable power level to combat it. We formulate a three-layer Stackelberg game to express the cooperation between the cellular user and all D2D users, and the confrontation between legitimate users and the active eavesdropper. We further propose two hybrid learning algorithms based on BR and SLA to obtain the pure-strategy and the mixed-strategy Stackelberg equilibrium. The utility of all D2D users versus the self-interference factor of the active eavesdropper is shown is Fig. 5. We can see that the utility of all D2D users decreases with the increasing of the self-interference factor of the full-duplex active eavesdropper and the proposed hybrid learning algorithms both present better performance than the RSA algorithm (Fig. 6).

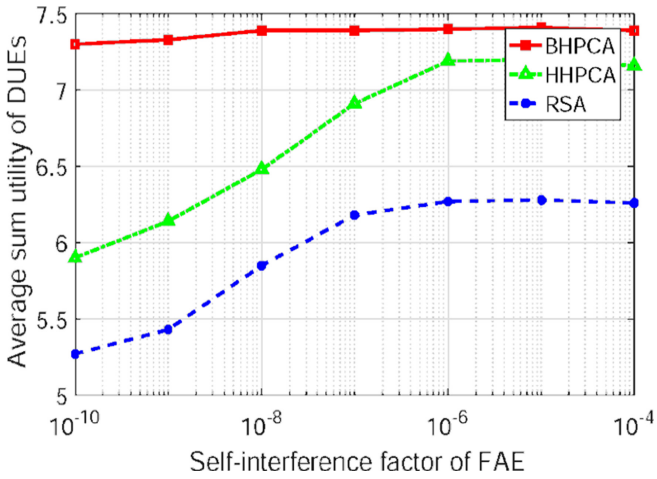

Fig. 6. Utility of D2D users versus self-interference of the full-duplex active eavesdropper

4.3 Smart Jamming Scenario

We also make some simulations under smart jamming scenario, which is shown in Fig. 3, where there exists an eNB, a cellular user, a smart jammer and some candidate D2D relay users. The coordinates of eNB and the cellular user are $(0\,\text{km}, 10\,\text{km})$ and $(10\,\text{km}, 0\,\text{km})$. The smart jammer is located in $(10\,\text{km}, 10\,\text{km})$. There are 4 D2D users, which are located in $(2.5\,\text{km}, 2.5\,\text{km})$, $(5\,\text{km}, 2.5\,\text{km})$, $(5\,\text{km}, 5\,\text{km})$, $(7.5\,\text{km}, 5\,\text{km})$ respectively. Considering that the smart jammer can select its jamming strategy according to listening messages, the legitimate transmitter and the selected relay can intelligently modify their transmission power to anti-smart jamming of this kind. The hierarchical interactions among different users is formulated as a Stackelberg game, and a hybrid learning algorithm based on Q learning and multi-armed bandit (MAB) is

proposed, and the performance of legitimate users is compared with the random selecting algorithm with different eavesdropping errors is shown in Fig. 7.

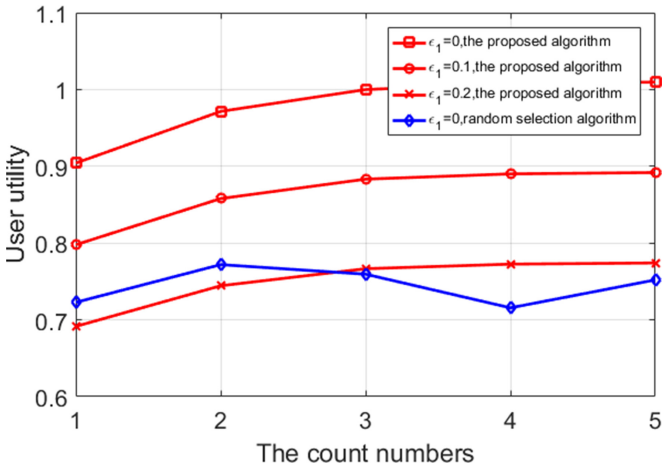

Fig. 7. Utility of legitimate users versus time slots with eavesdropping error of an active jammer

From all numerical results shown above, the game-theoretic learning approaches are available for legitimate users to improve the physical layer security and anti-jamming performance under active attacks.

5 Future Research Directions

We have discussed the physical layer security and anti-jamming problems in D2D communications under different attacking scenarios in previous sections. It has been verified that game-theoretic learning methods were feasible and effective to combat active attackers, and some research results have been achieved to improve anti-eavesdropping and anti-jamming performance of legitimate users. However, in view of complex interactions among different agents and information uncertainty of electromagnetic environment, there are a lot of open issues to be solved. Then we analyze the future research directions on secure and reliable D2D communications when facing with active attackers.

Practical Cooperation Mechanisms and Technologies of Legitimate Users: To confront active attackers, necessary cooperation among legitimate users is needed, not only among D2D users, but also between cellular users and D2D users. Some researches have introduced social relationship into D2D communications, how to employ social relationship among D2D users to further improve security performance and transmission reliability with intelligent attackers is worth to study. Moreover, considering the hierarchical characteristic between cellular users and D2D users, how to design the hierarchical cooperation mechanism is a future research direction. Due to

emerging technologies of 5G, such as non-orthogonal multiple access (NOMA), multiple antenna technology, millimeter-wave (mmWave) communications and unmanned aerial vehicle (UAV) enabled communications, transmission efficiency and security of wireless communications can be enhanced accordingly. Take the example of UAV enabled communications, from the perspective of the physical layer security, UAVs can work as mobile relays or friendly jammers to help improve anti-eavesdropping performance of massive machine-type devices. Recently, there are few works on secure and reliable communications by the aid of these emerging technologies against active attackers. Therefore, it will be an open issue to introduce them into combating intelligent attackers.

Tradeoff of Offensive and Defensive of Active Attackers: From the standpoint of active attackers, they want to maximize the destruction to legitimate users and unlikely to be discovered. On one hand, when they work as passive eavesdroppers, they can only wiretap confidential information and hard to be discovered. On the other hand, they can do much more harm to legitimate users when they work as active jammers, while can be easier to be found since they need to transmit vicious jamming signals. So there exists a tradeoff of offensive and defensive of active attackers, how to apply flexible attack strategies to maximize their destruction to legitimate users and hide their positions will be an open issue.

Massive D2D Communications Modeling and Multi-tier and Heterogeneous Game Formulation: At the present, the scheme that legitimate users cooperate with each other to maximize their utilities have been studied under game theory frameworks. But when the number of active eavesdroppers or legitimate users becomes very large, how to model their interactions using game theory and how to obtain the stationary or optimal equilibrium solutions will be a huge challenge. On one hand, the mean field game, which is a kind of differential game, can be applied to model group behavior of a huge number of players and describe the influence of crowd behavior on the individual agent. While due to dynamic changes of attacking strategies, how to quickly obtain stationary states of the mean field game will be a new challenge. On the other hand, considering complex interactions among cellular users, D2D users and intelligent attackers, multi-tier Stackelberg game should be formulated to improve security and reliability of legitimate users. Whether the equilibrium of multi-tier game exists should be discussed and the existence condition should be further analyzed.

Optimization with Incomplete Information and Applications of Deep Reinforcement Learning: Since the positions of legitimate users and intelligent attackers are competitive, there are no information exchanges between them. They only make their decisions based on imperfect information for each other. There have been some researches on the physical layer security or anti-jamming problem based on limited observations, while with no information on the opposite side, how to maximize their utilities based on machine learning methods is an issue worthy of studying. The deep reinforcement learning methods are suitable for solving the problem under such situation and don't need to apply under a special game framework. Based on deep reinforcement learning methods, intelligent users can update their power and channel selections according to training data without any information on attackers' utilities and

strategy sets. Deep reinforcement learning methods have just been used to confront smart jammers, while how to accelerate convergence of deep reinforcement learning methods are really an open issue.

6 Conclusion

In this paper, we have analyzed security threats in D2D underlaying cellular networks under different attacking scenarios. Based on hierarchical game framework, we expound the optimization objective description, utilities design and strategies selection of cellular users and D2D users. Furthermore, we have illustrated kinds of machine learning methods, such as fictitious play, MAB, Q-learning and SLA, to optimize transmission power, relay selection and other strategies to improve the physical layer security and anti-smart jamming performance. Finally, the future directions and challenges were discussed.

References

1. Ahmed, K.-I., Tabassum, H., Hossain, E.: Deep learning for radio resource allocation in multi-cell networks. IEEE Network Early Access **33**(6), 188–195 (2019)
2. Nawaz, S.-J., Sharma, S.-K., Wyne, S., Patwary, M.-N., Asaduzzaman, M.: Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future. IEEE Access **7**, 46317–46350 (2019)
3. Alrowaily, M., Lu, Z.: Secure edge computing in IoT systems: review and case studies. In: 2018 IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, pp. 440–444 (2018)
4. Zhang, P., Niu, K., Tian, H., Nie, G.-F., Qi, Q., Zhang, J.: Technology prospect of 6G mobile communications. J. Commun. **40**(1), 141–148 (2019)
5. Sim, G.-H., Klos, S., Asadi, A., Klein, A., Hollick, M.: An online context-aware machine learning algorithm for 5G mmWave vehicular communications. IEEE/ACM Trans. Networking **26**(6), 2487–2500 (2018)
6. Hamamreh, J.-M., Arslan, H.: Joint PHY/MAC layer security design using ARQ with MRC and null-space independent, PAPR-aware artificial noise in SISO systems. IEEE Trans. Wireless Communications **17**(9), 6190–6204 (2018)
7. Zheng, G., Krikidis, I., Li, J., Petropulu, A.P., Ottersten, B.: Improving physical layer secrecy using full-duplex jamming receivers. IEEE Trans. Signal Process. **61**(20), 4962–4974 (2013)
8. Geraci, G., Egan, M., Yuan, J., Razi, A., Collings, I.-B.: Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding. IEEE Trans. Commun. **60**(11), 3472–3482 (2012)
9. Zou, Y.-L., Champagne, B., Zhu, W.-P., Hanzo, L.: Relay-selection improves the security-reliability tradeoff in cognitive radio systems. IEEE Trans. Commun. **63**(1), 215–228 (2015)
10. Tang, X., Ren, P.-R., Wang, Y.-C., Han, Z.: Combating full-duplex active eavesdropper: a hierarchical game perspective. IEEE Trans. Commun. **65**(3), 1379–1395 (2017)
11. Abedi, M.-R., Mokari, N., Saeedi, H., Yanikomeroglu, H.: Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: active adversary. IEEE Trans. Wireless Commun. **16**(2), 885–899 (2017)

12. Li, L., Petropulu, A.-P., Chen, Z.: MIMO secret communications against an active eavesdropper. IEEE Trans. Inf. Forensics Secur. **12**(10), 2387–2401 (2017)
13. Qu, J., Cai, Y., Zheng, J., Yang, W., Wu, D., Hu, Y.: Power allocation for device-to-device communication underlaying cellular networks under a probabilistic eavesdropping scenario. Ann. Telecommun. **71**(7), 389–398 (2016). https://doi.org/10.1007/s12243-016-0515-x
14. Mei, W.-D., Chen, Z., Fang, J., Fu, B.: Secure D2D-enabled cellular communication against selective eavesdropping. In: IEEE ICC 2017 Communication and Information System Security Symposium, pp. 1–6 (2017)
15. Mukherjee, A., Swindlehurst, A.-L.: Jamming games in the MIMO wiretap channel with an active eavesdropper. IEEE Trans. Signal Process. **61**(1), 82–91 (2013)
16. Luo, Y., Yang, Y., Duan, Y., Yang, Z.: Joint D2D cooperative relaying and friendly jamming selection for physical layer security. In: Meng, L., Zhang, Y. (eds.) MLICOM 2018. LNICST, vol. 251, pp. 115–126. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00557-3_12
17. Luo, Y.-L., Feng, Z., Jiang, H., Yang, Y., Huang, Y., Yao, J.: Game-theoretic learning approaches for secure D2D communications against full-duplex active eavesdropper. IEEE Access **7**, 41324–41335 (2019)
18. Yang, D., Xue, G., Zhang, J., Richa, A., Fang, X.: Coping with a smart jammer in wireless networks: a Stackelberg game approach. IEEE Trans. Wireless Commun. **12**(8), 4038–4047 (2013)
19. Xu, Y., et al.: A one-leader multi-follower Bayesian-Stackelberg game for anti-jamming transmission in UAV communication networks. IEEE Access **6**, 21697–21709 (2018)
20. Yu, L., Wu, Q., Xu, Y., Ding, G., Jia, L.: Power control games for multi-user anti-jamming communications. Wireless Netw. **25**(5), 2365–2374 (2018). https://doi.org/10.1007/s11276-018-1664-9
21. Tang, X., Ren, P., Wang, Y., Du, Q., Sun, L.: Securing wireless transmission against reactive jamming: a Stackelberg game framework. In: Proceeding of IEEE GLOBECOM, pp. 1–6 (2015)
22. Wu, Y., Wang, B., Liu, K.J.R., Clancy, T.C.: Anti-jamming games in multi-channel cognitive radio networks. IEEE J. Sel. Areas Commun. **30**(1), 4–15 (2012)
23. Liu, X., Xu, Y., Jia, L., Wu, Q., Anpalagan, A.: Anti-jamming communications using spectrum waterfall: a deep reinforcement learning approach. IEEE Commun. Lett. **22**(5), 998–1001 (2018)
24. Feng, Z.-B., et al.: Power control in relay-assisted anti-Jamming systems: a Bayesian three-layer Stackelberg game approach. IEEE Access **7**, 14623–14636 (2019)
25. Song, L., Niyato, D., Han, Z., Hossain, E.: Game-theoretic resource allocation methods for device-to-device communication. IEEE Commun. Mag. **21**(3), 136–144 (2014)
26. Wang, F., Song, L., Han, Z., Zhao, Q., Wang, X.: Joint scheduling and resource allocation for device-to-device underlay communication. In: IEEE Wireless Communication and Networking Conference (WCNC), pp. 1–6 (2013)
27. Chu, Z., et al.: Game theory based secure wireless powered D2D communications with cooperative jamming. In: Wireless Days, pp. 95–98 (2017)
28. Luo, Y.-J., Yang, Y., Cui, L.: Research on physical layer security in D2D enabled cellular networks with an active eavesdropper. Sig. Process. **34**(1), 119–125 (2018)
29. Tang, X., Ren, P., Han, Z.: Power-efficient secure transmission against full-duplex active eavesdropper: a game-theoretic framework. IEEE Access **5**, 24632–24645 (2017)
30. Huang, W., Chen, W., Bai, B., Han, Z.: Wiretap channel with full-duplex proactive eavesdropper: a game theoretic approach. IEEE Trans. Veh. Technol. **67**(8), 7658–7663 (2018)

31. Fang, H., Xu, L., Zou, Y., Wang, X., Choo, K.R.: Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication. IEEE Trans. Veh. Technol. **67**(11), 10788–10799 (2018)
32. Luo, Y.-J., Yang, Y.: D2D friendly jamming and cooperative relaying for combating a full-duplex active eavesdropper. In: ICCT 2019, pp. 1–6 (2019)
33. Jia, L., Yao, F., Sun, Y., et al.: Bayesian Stackelberg game for anti-jamming transmission with incomplete information. IEEE Commun. Lett. **20**(10), 1991–1994 (2016)
34. Li, Y., Xiao, L., Liu, J., et al.: Power control Stackelberg game in cooperative anti-jamming communications. In: International Conference on Game Theory for Networks, pp. 1–6 (2015)
35. Jia, L., Yao, F., Sun, Y., et al.: A hierarchical learning solution for anti-jamming Stackelberg game with discrete power strategies. IEEE Wirel. Commun. Lett. **6**(6), 818–821 (2017)
36. Feng, Z., et al.: An anti-Jamming hierarchical optimization approach in relay communication system via Stackelberg game. Appl. Sci. **9**, 1–14 (2019)