ACCEPTED FROM OPEN CALL

Stackelberg Game Approaches for Anti-Jamming Defence in Wireless Networks

Luliang Jia, Yuhua Xu, Youming Sun, Shuo Feng, and Alagan Anpalagan

Abstract

This article investigates the anti-jamming communications problem in wireless networks from a Stackelberg game perspective. By exploring and analyzing the inherent characteristics of the anti-jamming problem, we present and discuss some technical challenges and fundamental requirements to address them. To be specific, the adversarial characteristic, incomplete information constraints, dynamics, uncertainty, dense deployment, and heterogeneous feature bring technical challenges to anti-jamming communications in wireless networks. Then, for the purpose of improving system performance, four requirements for anti-jamming communications are presented and discussed. Following the advantages of the Stackelberg game model in the anti-jamming field, we formulate an anti-jamming decision-making framework based on the Stackelberg game for anti-jamming defence in wireless networks. Moreover, two preliminary case studies are presented and discussed for better understanding of the anti-jamming Stackelberg game problem. Finally, some future research directions are also provided.

Introduction

Due to the shared and broadcast nature, wireless transmission is highly vulnerable to various attacks, such as spoofing attacks, eavesdropping attacks, data falsification attacks, jamming attacks, and so on. Therefore, security becomes a critical attribute of wireless networks, and has attracted extensive attention in the past decade. In this article, we focus on jamming attacks [1, 2, 3], which are a serious threat to the security of wireless networks, and deteriorates system performance significantly. The anti-jamming problem is an interesting and challenging topic in wireless transmission, and also a vital issue for the security of spectrum availability. Various countermeasures have been proposed to fight against jamming attacks, and they can be broadly classified into two types: spread spectrum based techniques and resource allocation based techniques [4]. However, spread spectrum based techniques, such as Frequency Hopping Spread Spectrum (FHSS), Uncoordinated Frequency Hopping (UFH), and Random Codekey Selection using Codebook DSSS (RCSC DSSS)[3], require wideband spectrum, and therefore are regarded to be spectrally inefficient. It is of great importance to develop anti-jamming schemes that have efficient spectral efficiency, especially in scarce spectrum scenarios. Thus, it motivates the optimal resource allocation based techniques (i.e., game theory based methods [5–13]), which constitute another family of anti-jamming methods and try to obtain effective use of resources. Moreover, with the development of cognitive radio technology and artificial intelligence, jamming attacks with higher-level intelligence pose a great challenge to the existing defence mechanisms. Therefore, it is extremely important and timely to develop efficient and flexible anti-jamming schemes.

Game theory is a powerful mathematical tool to adequately model and analyze the mutual interactions among players. Among the game theoretical models, Stackelberg game, as an important hierarchical game, stands out to capture the sequential interactions among players, and to make strategic decision-making in wireless networks. Considering the different attributes and hierarchical behaviors of legitimate users and jammers, Stackelberg game is a promising method to analyze the hierarchical interaction process between legitimate users and jammers, and it is, therefore, a suitable framework for the sequential decision-making of the anti-jamming defence in wireless networks. The advantages for exploiting Stackelberg game in the anti-jamming field are given as follows:

•Legitimate users and jammers belong to different identities, and they have different attributes. Stackelberg game can capture the interactions among players with different attributes. Moreover, legitimate users need to detect the jammers' actions to combat jammers, or the jammers are able to learn users' strategies to improve jamming efficiency. Thus, the anti-jamming problem contains a natural hierarchical characteristic, and Stackelberg game is a suitable framework to capture and analyze the hierarchical interactions between legitimate users and jammers.

•Competitive interactions exist between legitimate users and jammers (upper-level players and lower-level players), and mutual competitive interactions also exist among legitimate users (players with the same level) in dense wireless networks. Fortunately, the Stackelberg game model can simultaneously capture the competition at different levels.

The Stackelberg game model has attracted growing attention in the anti-jamming field recently, and some Stackelberg game solutions have been presented for anti-jamming defence in wire-

Digital Object Identifier:
10.1109/MWC.2017.1700363

Luliang Jia, Yuhua Xu (corresponding author), Youming Sun, Shuo Feng are with the Army Engineering University of PLA; Luliang Jia is also with Space Engineering University ; Alagan Anpalagan is with Ryerson University.

1536-1284/18/$25.00 © 2018 IEEE

less communications. In [5–9], the Stackelberg game framework was employed to model and analyze the transmitting-jamming problem, and the anti-jamming power control game was investigated in wireless networks. In [10], the cooperative transmission game was studied, and the equilibrium solution was obtained. In [11], the authors formulated an attacker-defender Stackelberg game between a jammer and a target node, and the timing channel was exploited. In [12], a secure offloading game was formulated, and the Stackelberg equilibrium was derived. In [13], we investigated the anti-jamming channel selection problem in an adversarial environment, and proposed a hierarchical learning approach to obtain desirable solutions.

Note that a survey of the jamming and anti-jamming techniques in wireless networks can be found in [2]. It investigated several types of jammers from the jamming point-of-view and summarized the existing anti-jamming techniques from the perspective of system security. In this article, however, we investigate the anti-jamming defence problem in wireless networks from a Stackelberg game perspective, and we mainly focus on exploring and analyzing the inherent features, fundamental requirements and technical challenges in anti-jamming communications research. The main contributions of this article are given as follows:

- We analyze and discuss the fundamental requirements and technical challenges according to the inherent characteristics of the anti-jamming defence problem in wireless networks.
- We outline some advantages of the Stackelberg game for anti-jamming defence in wireless networks, and formulate an anti-jamming decision-making framework based on the Stackelberg game.
- We provide the future research directions of the anti-jamming defence in wireless networks.

The rest of the article is organized as follows. In the following section, we discuss and analyze the technical challenges and fundamental requirements of anti-jamming defence in wireless networks. Then the Stackelberg game-theoretic model is investigated, and an anti-jamming decision-making framework based on Stackelberg game is established. Following that, two preliminary case studies are given, and future research directions are discussed. Finally, concluding remarks are presented.

Challenges and Requirements for Anti-Jamming Communications in Wireless Networks

From the perspective of engineering, analogous to the cognition cycle, we formulate an anti-jamming communications cycle to describe the anti-jamming operations, which is the backbone of anti-jamming communications. As shown in Fig. 1, the anti-jamming communications cycle mainly consists of the following steps: jamming cognition, anti-jamming decision-making, and waveform reconfiguration.

Jamming Cognition: The anti-jamming communications cycle begins with jamming cognition, and cognitive radio technologies can be employed to acquire useful information. It can perceive jamming activities and a complicated surrounding environment. Specifically, it should include jammer detection, jammer localization, and so on. For jammer detection, many techniques have been proposed, such as machine learning, compressing sensing, and the estimation-based detection method. The existing detection approaches were proposed for specific network environments and jamming models. However, it is a challenging task to differentiate a jamming scenario for legitimate users due to the non-cooperative relationship between legitimate users and jammers. Jammer localization is another important aspect, and various methods were provided, such as range-based methods (e.g., Pinpoint, WiSlow, and CrowdLoc) and range-free methods (e.g., Centriod Localization, Double Circle Localization, and Triple Circles Localization). Due to the adversarial characteristic and environmental factors, inaccurate measurements and data insufficiencies are the main challenges in jammer localization. Note that jamming cognition is not limited to sensing the surrounding environment and obtaining useful information; it can also realize high-level intelligence in the near future, such as knowledge discovery and jamming prediction.

The anti-jamming communications cycle begins with jamming cognition, and cognitive radio technologies can be employed to acquire useful information. It can perceive jamming activities and a complicated surrounding environment. Specifically, it should include jammer detection, jammer localization, and so on.

Anti-Jamming Decision-Making: Based on jamming cognition, anti-jamming decision-making is performed in adversarial environments, and the optimal anti-jamming strategy (e.g., transmission power, channel) is chosen. It is the core technology of anti-jamming communications, and a challenging task is to make effective anti-jamming decision-making in wireless networks, especially in scarce resource scenarios and smart jammer scenarios. Due to the features of the wireless network and adversarial characteristic, the anti-jamming decision-making problem faces some challenges, which will be presented later. For anti-jamming decision-making, various techniques were proposed in existing literatures, such as game theory based techniques, multi-armed bandit based techniques, reinforcement learning based techniques, and so on. Among these methods, game theory based techniques, especially the Stackelberg game based techniques, can adequately model the interactions between legitimate users and jammers. In this article, we mainly analyze Stackelberg game based anti-jamming methods.

Waveform Reconfiguration: Waveform reconfiguration can be accomplished in multi-domains, such as the power domain, the spectrum domain and the space domain, to implement anti-jamming communications. It is the physical measure to achieve reliable transmission in jammed wireless networks. In the power domain, we can fight against jamming attacks by adjusting the transmitting power. However, the increase of transmitting power may deteriorate the linearity of the power amplifier, and it will affect the performance of some modulation schemes that are sensitive to the linearity of the power amplifier. In the spectrum domain, channel switching is adopted to cope with jamming attacks. Note that channel switching may cause performance loss, since the reconstruction of the communication link needs settling time for radio frequency (RF) devices. Moreover, different frequencies will have different propagation characteristics, and it may cause a difference in signal processing.

In this article, we mainly focus on the anti-jamming decision-making process, which is the critical phase anti-jamming communications in wireless networks. In the following, we aim to explore the inherent features of anti-jamming communications,

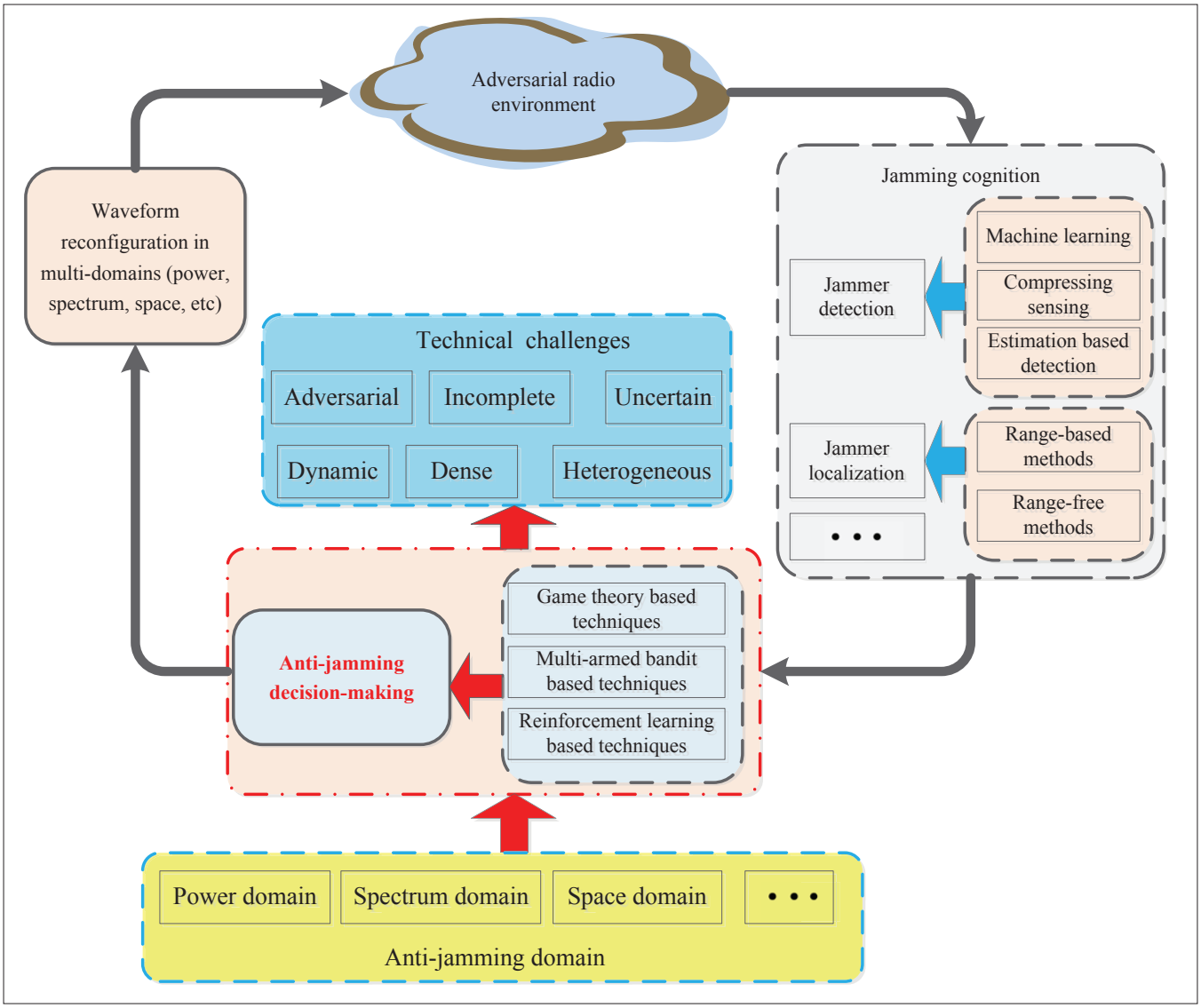

FIGURE 1. Anti-jamming communications cycle in wireless networks.

and we discuss and analyze the technical challenges and fundamental requirements of anti-jamming defence in wireless networks. In the following, we mainly consider the anti-jamming defence problem in the power domain and spectrum domain.

Discussion of Technical Challenges

For anti-jamming communications in wireless networks, it pursues the reliable transmission in the presence of external malicious jammers. In this section, by exploring the characteristics of wireless networks [14] and specificities in jammed networks, we discuss the technical challenges of the anti-jamming problem.

Adversarial: In jammed wireless networks, legitimate users always aim to maximize their utilities and pursue reliable transmission, whereas malicious jammers try to purposely deteriorate the intended transmission and minimize the utility of legitimate users. Therefore, legitimate users and jammers work in an adversarial and non-cooperative environment.

Different from general wireless networks, the adversarial characteristic is an important challenge in jammed networks. It is difficult to acquire complete information of the opponent due to the adversarial characteristic, and the incomplete information constraints are common in anti-jamming decision-making. To cope with the incomplete information constraints, the Bayesian game framework and learning technologies (i.e., stochastic learning automata) are effective methods. In a Bayesian game framework, the utility function is defined over statistics, such as taking expectation, to describe the incomplete information constraints, and only the distribution information is needed. Learning technology is another candidate to deal with incomplete information constraints. It can obtain desirable solutions by trial-and-error exploration and learning from historical information.

Incomplete: Due to the adversarial feature between legitimate users and jammers, it is difficult to acquire complete information about the opponents. Furthermore, considering the limitation of hardware and resource consumption, only partial information of the environment is available for both the users and jammers. Various forms of incomplete information constraints can be present, such as incomplete information of the channel gain [8] and the user type [15].

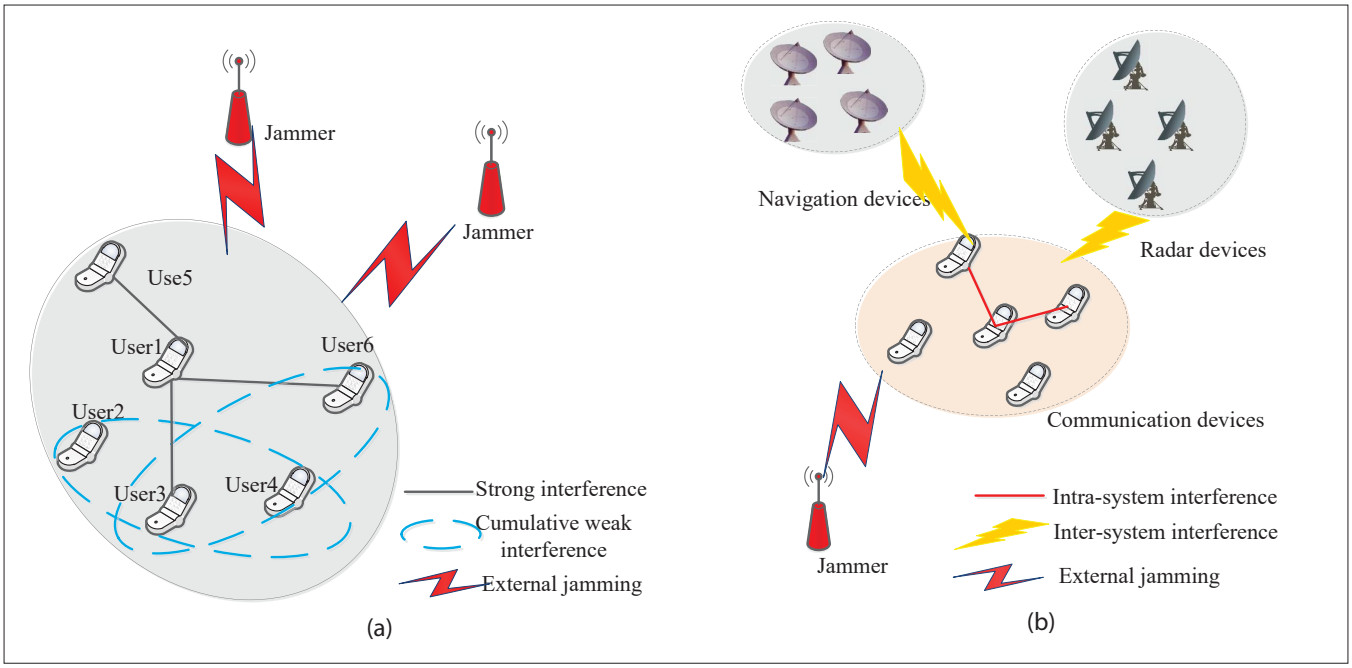

FIGURE 2. An illustration of the wireless networks: a) an illustration of the dense wireless networks; b) an example of the heterogeneous networks.

Uncertain: Due to the limitation of the capability of the signal processing and hardware facilities, it is difficult to observe perfect information, and the observation error is common in the anti-jamming field.

Dynamic: Environmental information is variable over the course of time. For example, channel state information is dynamic, and traffic demands are time-varying due to their specific requirements. Furthermore, the position of the jammers may be random as well.

Dense: In the future, dense networks will common, such as small cell networks and D2D networks. It will be challenging and interesting to investigate the anti-jamming problem in dense wireless networks, where both the mutual interference among users and external malicious jamming need to be simultaneously considered. Specifically, external jamming is a crucial factor that leads to performance degradation, and mutual interference among users is another factor that significantly restricts network performance.

For the anti-jamming problem in dense networks, first it is of paramount importance to fight against external malicious jamming. Second, it is essential to consider the interference mitigation problem. In our prior work [13], a preliminary anti-jamming scheme in dense wireless networks had been investigated, and a hierarchical learning framework was formulated. It is noted that the hypergraph model is a good candidate to explicitly describe the interference relation. As can be seen from Fig. 2a, the hypergraph interference model can adequately capture the strong interference relation and cumulative weak interference relation. The dash lines in Fig. 2a represent the strong interference relation, and the circles denote the cumulative weak interference relation. It will be promising to incorporate the hypergraph interference model into the anti-jamming game in dense wireless networks.

Heterogeneous: In future wireless networks, as indicated in Fig. 2b, different types of devices will co-exist in a region, such as communication devices, navigation devices, radar devices, and so on. It will lead to a severe conflict and complicated environment. Intra-system interference, inter-system interference, and external malicious jamming need to be jointly considered.

In heterogeneous wireless networks, there exist diverse devices. Meanwhile, different devices belong to different systems (e.g., communication, navigation, and radar), and have different service demands (e.g., voice, image, and data). Different systems and services may have different anti-jamming requirements. Moreover, due to the dense deployment of diverse devices, severe intra-system interference and inter-system interference present new challenges. Therefore, it will be extremely challenging to investigate the anti-jamming problem in heterogeneous wireless networks, and we need to jointly cope with intra-system interference, inter-system interference, and external malicious jamming.

Discussion of Fundamental Requirements

Considering the inherent characteristics, we list some fundamental requirements of the anti-jamming defence problem in wireless communications, which mainly include reliability, robustness, scalability, and heterogeneity.

First, it is necessary to obtain reliable transmission in wireless networks, and design effective anti-jamming approaches, especially in scarce resource scenarios and smart jammer scenarios.

Second, it should be robust to cope with different kinds of dynamics and uncertain factors in the anti-jamming field. As discussed before, channel state information is partially available. Moreover, traffic demands may be variable.

Third, as stated before, user devices will be densely deployed in future wireless networks, and both mutual interference and external jamming will affect system performance. Therefore, the designed anti-jamming defence schemes should

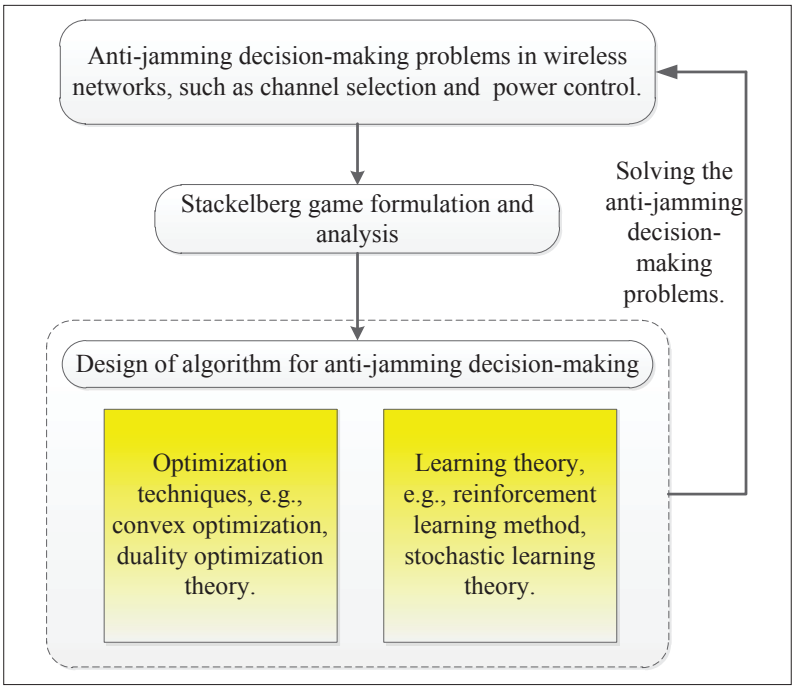

FIGURE 3. The proposed anti-jamming decision-making framework in wireless networks.

have the ability to be extended to dense scenarios, and address mutual interference among users and malicious jamming simultaneously.

Finally, various heterogeneous devices will coexist in future wireless networks. This presents new challenges to traditional anti-jamming solutions in homogeneous networks, and they cannot be directly employed. Therefore, it is essential to develop novel anti-jamming schemes in heterogeneous wireless networks.

Anti-Jamming Stackelberg Game in Wireless Networks

The Stackelberg game is regarded as an extension of the non-cooperative game, and it is a powerful mathematical tool that can be used to model the hierarchical interactions among players in a sequential manner. In a Stackelberg game, there are two types of players: leaders and followers. The leaders have priority over the followers and take actions first. Then, the followers make decisions based on the leaders' announced strategy. For a Stackelberg game model, the leaders and followers have their respective utility functions, and the most common solution is the Stackelberg Equilibrium (SE), which means no player can achieve higher utility by deviating unilaterally.

The Stackelberg game model has been extensively applied to wireless networks recently, and it has been a powerful tool to make hierarchical decision-making in wireless networks, such as the offloading mechanism, enhancing the secrecy rate, dynamic spectrum access in heterogeneous networks, wireless service provider selection, and power control in femtocell networks. In the anti-jamming field, it is an appealing tool to adequately model and analyze the hierarchical interactions between legitimate users and external jammers, and make strategic decisions in an adversarial environment.

To deal with the technical challenges of the anti-jamming issue in wireless networks, an anti-jamming decision-making framework based on Stackelberg game is formulated to combat jammers. As shown in Fig. 3, it mainly consists of two steps:

- Stackelberg game formulation and analysis.
- Design of algorithms for anti-jamming decision-making.

Stackelberg Game Formulation and Analysis: First, it is necessary to recognize the identities and their available actions of the players, and design proper utility functions accordingly. Second, for an anti-jamming Stackelberg game, we need to ask who acts as the leaders and who are the followers, the answer to which is that it depends on specific research scenarios. For example, in [5, 6, 8, 9], it is assumed that the jammer is able to learn the legitimate user's strategies, and legitimate users take action first. The legitimate user is the leader, and the jammer is assumed to be the follower. In [7], two scenarios (jammer as the leader and user as the leader) are both considered. In [13], the users need to detect the jammer's actions before channel selection, and it is assumed that the jammer acts as the leader and the users are followers. Since the utility function has a great impact on the performance of the game model, it is thus important to define proper utility functions. For example, the player can obtain the unique optimal strategy for the power control problem if the utility function is convex [8]. For the channel selection problem, the properties of the game model depend on the utility function, such as the exact potential game, which satisfies that the variation of the potential function is the same as the variation of the utility function by any player's unilateral deviation. The exact potential game has several attractive properties (i.e., admitting at least one pure strategy Nash equilibrium), and it can be incorporated into the follower sub-game [13].

Mathematically, an anti-jamming Stackelberg game can be formulated as $\mathcal{G} = \{\mathcal{N}_u, \mathcal{N}_j, \mathcal{S}_u, \mathcal{S}_j, \mu_s, \mu_j\}$, where $\mathcal{N}_u$ and $\mathcal{N}_j$, $\mathcal{S}_u$ and $\mathcal{S}_j$, μ_s and μ_j are player set, strategy space, and utility function of the legitimate users and jammers, respectively. In a Stackelberg game model, there exists a hierarchical competition between the upper-level players (leaders) and lower-level players (followers). Moreover, mutual competition also takes place among the players within the same level. Fortunately, the Stackelberg game can adequately model and analyze the competition at different levels.

The Bayesian Stackelberg game is a good framework to cope with the uncertainties due to the uncertain and incomplete constraints. For the dense deployment scenario, Stackelberg game is a suitable tool that can analyze the mutual competition among legitimate users and the competition between legitimate users and external jammers simultaneously. For a future heterogeneous network, intra-system interference, inter-system interference, and external malicious jamming co-exist, and the multi-level Stackelberg game may be a good candidate for the anti-jamming problem in heterogeneous wireless networks.

Design of Algorithms for Anti-Jamming Decision-Making: For the anti-jamming Stackelberg game problem, it is also a hierarchical optimization problem, and can be transformed into sequential

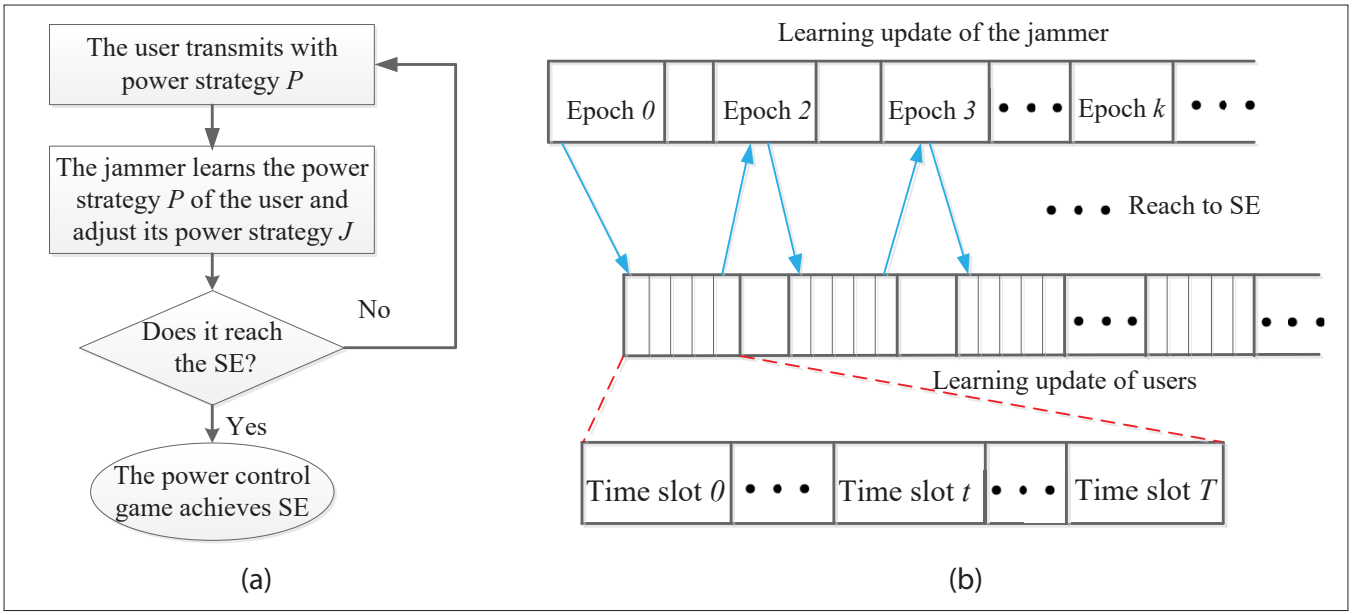

FIGURE 4. The implementation process of the anti-jamming Stackelberg game: a) the process of the anti-jamming power control game; b) the process of anti-jamming channel selection game.

sub-problems. To achieve this, a backward induction method is a common approach, and it has been employed to analyze the Stackelberg game and obtain game-theoretic solutions. The follower sub-game is first investigated, then the leader sub-game is considered.

For the continuous problem, such as continuous power control [5–8, 10], the SE solution is obtained based on convex optimization techniques, such as Lagrange duality optimization theory, and Karush-Kuhn-Tucker (KKT) conditions. However, for discrete problem, such as the anti-jamming channel selection problem [13], it is intractable to adopt traditional convex optimization techniques, and we need a new optimization framework and thus resort to learning theory, which achieves desirable solutions through repeated trial-and-error exploration with a random environment. Some learning algorithms can be found in previous works, such as reinforcement learning, stochastic learning automata, and spatial adaptive play [14]. Learning technology can cope with uncertain, dynamic, and incomplete information constraints, whereas game theory can adequately model and analyze mutual interactions among users. Therefore, it is promising to incorporate learning technologies into game theory. However, when the learning algorithms are incorporated into game theory, the challenge is to prove the convergence of the learning algorithms, which is application-dependent and will significantly differ for various applications.

Case Studies

In this section, we present two case studies of anti-jamming Stackelberg game approaches to motivate the readers and highlight the practicality of such approaches.

Power Control Game with Incomplete Information

Most existing anti-jamming Stackelberg power game approaches studied scenarios with complete information. However, scenarios with incomplete information are more general and practical in the anti-jamming field. In [8], we investigated the anti-jamming power control problem with incomplete information constraints in wireless communications. A system model with one user (transmitter-receiver pair) and one jammer is considered, and a Bayesian anti-jamming Stackelberg game is proposed, which can cope with the adversarial characteristic, incomplete information constraints. To capture the incomplete information constraints, the utility function is defined over statistics, such as taking expectation. Based on the duality optimization theory, the SE solution is derived. Moreover, the impact of the jammer's observation error ε is analyzed. The utility function of the user is defined as the signal to interference plus noise ratio considering the transmission cost. The jammer's utility function is also defined as a function of the signal to interference plus noise ratio and the transmission cost. In the considered scenario, the user aims to maximize its utility, and takes action first. The jammer can learn the user's transmission strategies, and play its best response strategy based on the user's announced strategy. The SE solution is obtained by the backward induction method, and the follower sub-game is investigated first. To better understand the process of the power control game, a flow chart is shown in Fig. 4a. In this section, the transmission rate can be defined as:

$$R = \log(1 + \delta), \tag{1}$$

where δ denotes the signal to interference plus noise ratio.

In Fig. 5, we show the performance comparison of the transmission rate for different solutions. To evaluate the performance, we compare the proposed Bayesian anti-jamming Stackelberg game with the average game, which is a modified game in [5] and only concerns the average value of the incomplete information, for example, channel state information and transmission cost. It can be seen that the transmission rate of the proposed game

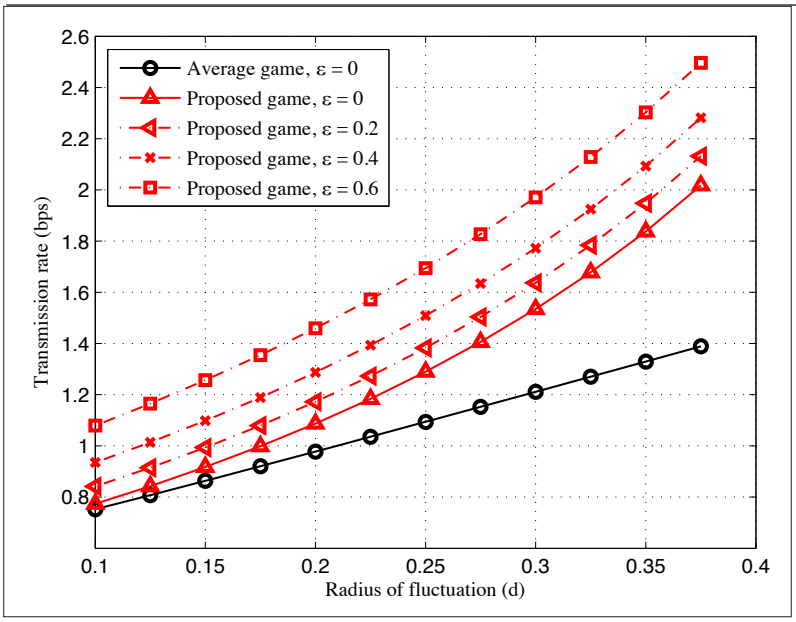

FIGURE 5. The performance comparison of different solutions.

is better than the average game. In addition, the observation error ε results in an increase of the user's transmission rate.

Anti-Jamming Channel Selection Game in Dense Wireless Networks

In this section, we investigate the anti-jamming channel selection problem in dense wireless networks with time-varying radio environments, where mutual co-channel interference among users and external malicious jamming exists simultaneously. On the one hand, external malicious jamming is a significant factor to deteriorate system performance of wireless networks. On the other hand, mutual co-channel interference also significantly degrades system performance. In [13], a system with N users and one jammer is considered, and a single leader and multi-follower Stackelberg game is formulated. To obtain desirable solutions, we propose a hierarchical learning algorithm (HLA), that can cope with uncertain, dynamic and incomplete constraints. The implementation process is shown in Fig. 4b. To be specific, for the jammer, based on Q-learning, a channel selection algorithm is proposed, and the jammer's strategies are updated at each epoch k. For users, a channel selection algorithm based on stochastic learning automata (SLA) is proposed, and the users' strategies update at each time slot t. It is noted that each epoch contains K time slots. The metric is the expected weighted aggregate interference and jamming (EWAIJ), and it is defined as:

$$U = \sum_{n\in\mathcal{N}} \sum_{m\in\{\mathcal{N}/\{n\}\}} P_n P_m \bar{H}_{mn}^{a_n} f(a_m, a_n) + \sum_{n\in\mathcal{N}} P_n P_j \bar{H}_{jn}^{c_j} f(c_j, a_n), \quad (2)$$

where a_n denotes the channel selection of user n, c_j denotes the jamming channel, $\mathcal{N}$ is the user set, $\bar{H}_{mn}^{a_n}$ represents the expected interference gain from user m to user n, $\bar{H}_{nj}^{c_j}$ denotes the expected jamming gain from the jammer to user n, $f(a_m, a_n)$ denotes an indicator function ($f(a_m, a_n) = 1$ for $a_m = a_n$, and $f(a_m, a_n) = 0$ for $a_m \neq a_n$), P_m and P_j represent the transmission power of user n and the jammer, respectively. The rate of user n can be given by:

$$R_n = B\log\left(1 + \frac{P_n H_{nn}^{a_n}}{BN_0 + I_n + J_n}\right) \quad (3)$$

where B denotes the bandwidth, N_0 is the noise power spectrum density, and I_n and J_n represent the co-channel interference and malicious jamming, respectively.

The utility of user n is defined as $u_n(a_n, \mathbf{a}_{-n}, c_j) = L - \Sigma_{m\in\{\mathcal{N}/\{n\}\}} P_n P_m \bar{H}_{mn}^{a_n} f(a_m, a_n) - P_n P_j \bar{H}_{jn}^{c_j} f(c_j, a_n)$, where L represents a predefined positive constant. Each user aims to maximize its utility. The jammer's utility is $u_j(\mathbf{a}, c_j) = \Sigma_{n\in\mathcal{N}} P_n P_j \bar{H}_{jn}^{c_j} f(c_j, a_n)$, and it aims at maximizing its damage. Our objective is to find a channel selection profile that can minimize EWAIJ, which denotes the received mutual interference and external malicious jamming.

In Fig. 6, the performance comparison is presented. To show the performance, we compare the proposed HLA algorithm with the random selection scheme, in which the user randomly selects one channel at each time. As indicated in Fig. 6a, the proposed HLA algorithm outperforms the random selection scheme, and higher transmitting power P_j of legitimate users results in the increase of the EWAIJ performance. Moreover, the EWAIJ increases with the growing number of users. The reason is that a growing number of users leads to more serious mutual interference. As can be seen from Fig. 6b, as the number of users increases, the expected achievable rate of each user decreases. The reason is that increasing the number of users causes heavy mutual interference. It is noted that the expected achievable rate grows with increasing transmitting power of users at first. Then, if the number of users is large enough, the curve would reach a steady level or even go downward with higher transmitting power of users. The reason is that higher transmitting power of legitimate users yields more serious mutual interference. As shown in Fig. 6c, the proposed HLA is superior to the random selection scheme and yields higher expected achievable rate. Specifically, when $N = 4$ and $P_j = 15$W, the expected achievable rate of the proposed HLA is improved by approximately 30 percent compared to the random selection scheme. It is also noted that the performance gap between the proposed HLA and random selection scheme decreases with the increasing number of users. The reason is that when the number of users N becomes sufficiently large, the channels are very crowded, and users can uniformly be spread over the channels. In addition, it can be seen from Fig. 6c that the expected achievable rate will decrease with the growing transmitting power of the jammer. The reason is that higher transmitting power of the jammer leads to more serious damage.

Future Research Directions

Although the study of anti-jamming schemes based on Stackelberg game is now in its infancy, it will definitely attract great interest and attention in the near future. Based on the previous discussions, we present some future research directions in the following.

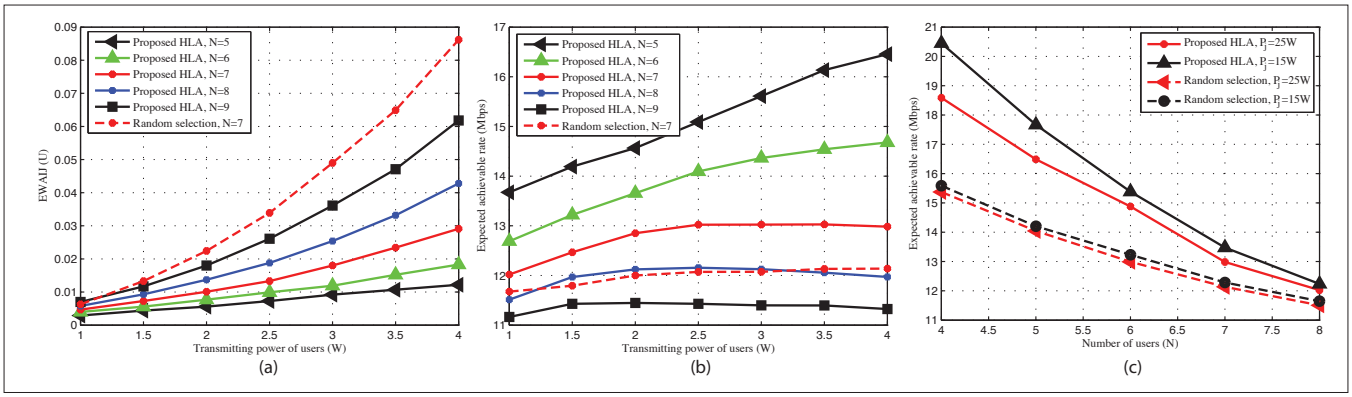

FIGURE 6. The performance comparison: a) comparison results of the EWAIJ (P_j = 25W); b) comparison results of the expected achievable rate (P_j = 25W); c) comparison results of the expected achievable rate for different solutions (P_n = 4W).

•To improve the jamming efficiency and decrease the probability of detection, the position of the jammer may be mobile in practical scenarios. Therefore, it is interesting to investigate anti-jamming problems in mobile scenarios.

•In realistic scenarios, the players' utility functions are not deterministic and random due to variable channel state information, noise, feedback errors, and observation error. It is, therefore, interesting to study the anti-jamming problem with estimation error. For this scenario, a noisy stochastic game can be formulated, and efficient estimation samples can be used to improve the anti-jamming performance.

•In dense wireless networks, we need to jointly consider mutual interference among legitimate users and external malicious jamming. Moreover, various traffic demands and priorities also need to be investigated. Specifically, different traffic demands will lead to a variable set of active users, and it results in a variable set of players. Thus, a dynamic game model with dynamic traffic demands is needed. Different priorities represent the degree of importance, and the users with higher priority should be satisfied with their requirements first. Consequently, it is promising to investigate anti-jamming schemes with dynamic traffic demands and different priorities in wireless networks.

•Considering the heterogeneity in future wireless networks, user devices may have various service demands and different anti-jamming requirements. Moreover, in a heterogeneous wireless network, intra-system interference, inter-system interference, and external malicious jamming co-exist, and therefore constitute a complicated environment. Thus, it is a challenging task to design anti-jamming approaches in heterogeneous wireless networks.

•According to the history observations of external jammers, we can predict the action of the jammers, and further enhance anti-jamming performance. Therefore, it is an interesting topic to design effective anti-jamming schemes with jamming prediction ability in future work.

Conclusion

In this article, we investigated the anti-jamming defence problem in wireless communications, which is an important topic in wireless transmission, and also a vital problem for the security of spectrum availability. First, we presented the technical challenges and fundamental requirements of the anti-jamming defence problem in wireless networks. Then, following the advantages of the Stackelberg game model in the anti-jamming field, an anti-jamming decision-making framework based on Stackelberg game was established. We provided two case studies to analyze an anti-jamming Stackelberg game. Finally, we proposed some future research directions.

Acknowledgments

This work was supported in part by the Natural Science Foundation for Distinguished Young Scholars of Jiangsu Province under Grant BK20160034; in part by the National Science Foundation of China under Grant 61631020, Grant 61671473, and Grant 61771488; and in part by the Open Research Foundation of Science and Technology in Communication Networks Laboratory.

References

[1] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming Games in Wireless Networks with Incomplete Information," *IEEE Commun. Mag.*, vol. 49, no. 8, Aug. 2011, pp. 112–18.
[2] K. Grover, A. Lim, and Q. Yang, "Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey," *Int'l. J. Ad Hoc and Ubiquitous Comput.*, vol. 17, no. 4, Dec. 2014, pp. 197–215.
[3] B. Gopalakrishnan and M. A. Bhagyaveni, "Random Codekey Selection Using Codebook without Pre-Shared Keys for Anti-Jamming in WBAN," *Computers and Electrical Engineering*, vol. 51, Apr. 2016, pp. 89–103.
[4] L. Zhang, Z. Guan, and T. Melodia, "United Against the Enemy: Antijamming Based on Cross-Layer Cooperation in Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 15 , no. 8, Aug. 2016, pp. 5733–47.
[5] D. Yang *et al.*, "Coping with a Smart Jammer in Wireless Networks: A Stackelberg Game Approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, Aug. 2013, pp. 4038–47.
[6] L. Xiao *et al.*, "Anti-Jamming Transmission Stackelberg Game with Observation Errors," *IEEE Commun. Lett.*, vol. 19, no. 6, June 2015, pp. 949–52.
[7] F. Slimeni *et al.*, "Optimal Power Allocation over Parallel Gaussian Channels in Cognitive Radio and Jammer Games," *IET Commun.*, vol. 10, no. 8, Feb. 2016, pp. 980–86.
[8] L. Jia *et al.*, "Bayesian Stackelberg Game for Anti-Jamming with Incomplete Information," *IEEE Commun. Lett.*, vol. 20, no. 10, Oct. 2016, pp. 1991–94.
[9] L. Jia *et al.*, "A Hierarchical Learning Solution for Antijamming Stackelberg Game with Discrete Power Strategies," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, Dec. 2017, pp. 818–21.
[10] L. Xiao *et al.*, "Power Control with Reinforcement Learning in Cooperative Cognitive Radio Networks against Jamming," *J. Supercomputing*, vol. 71, no. 9, Apr. 2015, pp. 1–21.
[11] S. D'Oro *et al.*, "Defeating Jamming with the Power of Silence: A Game-Theoretic Analysis," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, May 2015, pp. 2337–52.
[12] L. Xiao *et al.*, "A Mobile Offloading Game against Smart Attacks," *IEEE Access*, vol. 4, May 2016, pp. 2281–91.

[13] F. Yao *et al.*, "A Hierarchical Learning Approach to Anti-Jamming Channel Selection Strategies," *Wireless Netw.*, DOI: 10.1007/s11276-017-1551-9.
[14] Y. Xu *et al.*, "A Game-Theoretic Perspective on Self-Organizing Optimization for Cognitive Small Cells," *IEEE Commun. Mag.*, vol. 53, no. 7, July 2015, pp. 100–08.
[15] Y. E. Sagduyu, R. Berry, and A. Ephremides, "MAC Games for Distributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types," *Proc. GameNets 2009*, pp. 130–39.

Biographies

Luliang Jia (jiallts@163.com) received his B.S. degree in communications engineering from Lanzhou Jiaotong University, Lanzhou, China, in 2011, and the M.S. degree in communications and information systems from the College of Communication Engineering, PLA University of Science and Technology, Nanjing, China, in 2014. He is currently working toward the Ph.D. degree at the College of Communication Engineering, Army Engineering University of PLA. His current research interests include game theory, learning theory and communication anti-jamming technology.

Yuhua Xu (yuhuaenator@gmail.com) received his B.S. degree in communications engineering, and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, in 2006 and 2014, respectively. He is currently with the College of Communications Engineering, Army Engineering University of PLA. His research interests focus on opportunistic spectrum access, UAV communication networks, and game theory. He was selected to receive the IEEE Signal Processing Society's 2015 Young Author Best Paper Award, and the Funds for the Distinguished Young Scholars of Jiangsu Province in 2016.

Youming Sun (sunyouming10@163.com) received his B.S. degree in electronic and information engineering from Yanshan University, Qinhuangdao, China, in 2010, and the M.S. degree and Ph.D. degree from the National Digital Switching System Engineering & Technological Research Center (NDSC), Zhengzhou, China, in 2013 and 2016, respectively. His research interests focus on opportunistic spectrum access, learning theory, game theory, and distributed optimization techniques for wireless communications.

Shuo Feng (fengs13@mcmaster.ca) received the B.S. degree in electrical engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2011, and the M.Sc. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2014. His research interests include cognitive radio networks, machine learning, cognitive dynamic systems, and information geometry.

Alagan Anpalagan (alagan@ee.ryerson.ca) received the BASc., MASc. and Ph.D. degrees in electrical engineering from the University of Toronto. He is a registered Professional Engineer in the province of Ontario, Canada, a Senior Member of IEEE and a Fellow of the Institution of Engineering and Technology. He is a professor in the Department of Electrical and Computer Engineering at Ryerson University, where he directs a research group working on radio resource management (RRM) and radio access and networking (RAN) areas within the WINCORE Lab.