The Journal of Engineering

IET International Radar Conference (IRC 2018)

IET Journals
The Institution of Engineering and Technology

Performance analysis of one-step prediction-based cognitive jamming in jammer-radar countermeasure model

eISSN 2051-3305
Received on 28th May 2019
Accepted on 28th May 2019
E-First on 18th September 2019
doi: 10.1049/joe.2019.0916
www.ietdl.org

Lu Gao[1], Li Liu[2], Yang Cao[1], Shangyue Wang[1], Shixun You[3] ✉
[1]National Key Laboratory of Science and Technology on Test Physics and Numerical Mathematics, Beijing, People's Republic of China
[2]DFH satellite Co.,Ltd, Beijing, People's Republic of China
[3]Harbin Engineering University, 145 Nantong Street, Nangang District, Harbin, People's Republic of China
✉ *E-mail: gaolipeng@hrbeu.edu.cn*

Abstract: Strong adaptive radar, such as cognitive radar (CNR), can perform various missions while ensuring its own security in electronic warfare, via detecting environments and changing the radar parameters in real time. Unfortunately, most of the current military countermeasures, such as jamming-based electronic countermeasures, have rarely been related to jamming for CNR. Since the behaviours of radar in the traditional design of the jammer-radar scenario are always static, it is easy to create a subjective or local optimal jamming effect. In order to dynamically analyse the execution process of a complete jamming radar mission, this work establishes an equivalent attack-defence game in which the radar is regarded as a defence decision agent, and the jammer is an attack decision agent. The attributes of the game's players, the rules of the game, and the conditions for the end of the game are set clearly by setting reasonable parameters. After searching for antagonism strategies by exhaustive method, it can be found that the survivability of the predictive cognitive jamming is much stronger than that of the normal jamming based on real-time sampling data of radars. This conclusion is demonstrated through a 1 ms simulation of the game process.

1 Introduction

Currently, electronic warfare is the most colourful theatre in modern information warfare. The two most important roles on the stage, the radar and the jammer, have abilities that are evolving at the speed of superhuman imagination. Specifically, the complexity of the electromagnetic spectrum environment is the fundamental factor to promote this phenomenon. Thanks to the promotion of cognitive radio technology, the performance of cognitive radar (CNR) has been improved in many ways compared with the traditional radar. For example, cognitive radio can effectively enhance the dynamic management of the radar signal spectrum. It can also improve spectrum utilisation for a radar net. Additionally, the waveform adaptation allows the radar to obtain the best estimate of the target scatter coefficient, and the dynamic pulse repetition interval (PRI) of the radar can optimise the performance of different radar stages or modes.

The jammer-radar process is roughly divided into three phases including data acquisition, confrontation analysis, and the effect of evaluation-based jamming decision-making. The data acquisition is completed by the low-level system, and the ideal data can make the analysis easy to carry out. The confrontation analysis is used to evaluate the interactions between different jammers, radars, and jammer-radar pairs.

In recent years, the first phase of research, the identification of the radar emission sources, has been widely studied. Then, confrontation analysis was considered to be the key factor for evaluating jamming effects. Many researchers studied the effectiveness of jamming at the level of the electromagnetic spectrum (power, carrier frequency (CF), PRI etc.). For example, the authors in [1] used game theory to analyse the influences of different jamming technologies on the radar's detection performance, taking into account some adaptive radar response strategies. Similarly, some non-cooperative game-based jamming schemes designed in radar communication have gradually attracted many researchers [2–5]. However, the analysis of adaptive radar in these works is independent of different time intervals, in fact, from the perspective of continuous missions, the jamming produced by the last time interval may affect the jamming effect at the next. Fortunately, Osner and Plessis [6] designed a threat evaluation and jamming allocation system (TEJA) to achieve a jammer-radar process of a continuous 15 sampling cycles, in which the principles of the jamming decisions for each time interval were carefully analysed. The only drawback is that the target radars in the missions are not adaptive. It is worth noting that the system in [6] quantifies the interactions between jammers, and jammer-radar pairs via some user-defined look-up tables, which are not considered in traditional TEJA systems [7–9].

In this paper, we model a complete game to investigate the response strategies of the radar and the jammer in the confrontation process. The game is developed along a timeline, and it will continue to execute until one player of the game wins.

The details of the jammer-radar process are described in Section 2. We propose, in Section 3, an online game for the cognitive jammer to attack the CNR based on confrontation analysis, and in Section 4, the simulation and results of the game are displayed. In Section 5, some conclusions about cognitive jamming (CNJ) are presented.

2 Cognitive radar and jammers

Jammers automatically plan jamming strategies under the conditions allowed by electronic warfare systems. To solve this problem well, knowledge of various radars, jammers, and the electromagnetic spectrum needs to be considered.

2.1 Cognitive radar

The closed-loop feedback in a CNR system consists of the transmitter, the environment, and the receiver. CNRs can adaptively optimise the transmit waveform and improve the performance of target estimation, detection, and tracking based on the operating environment. On one hand, the signal-to-noise rate (SNR) of the echo waveform can be maximised by optimising the transmit waveform, which can further improve the target detection performance. On the other hand, since the information of the target impulse response can be estimated from the echo waveform, the

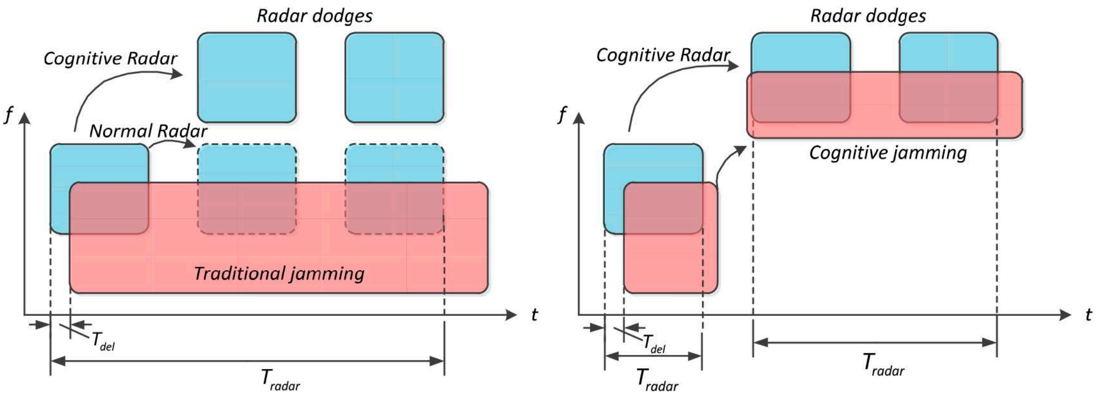

Fig. 1 *Illustration of the CNJ*

estimated performance can be improved by optimising the transmit waveform [10].

CNR is considered to be radar equipment that can change the parameters of the transmitter to maximise the radar performance through interaction with the operating environment [11]. Generally, radar parameters related to the electromagnetic spectrum, i.e. the radar characteristics, are mainly reflected in the frequency domain, energy domain, time domain, and polarisation domain. From the viewpoint of signal propagation, the spatial location for a radar is also significant.

This paper investigates a jamming operation scenario with a short time interval (in ms). It is assumed that the radar and the jammer are relatively static in the space, and their polarisation matches are not considered. Simultaneously, it is fair to assume that the radar can identify any jamming technology adopted by the jammer, and the jammer can also identify any stage or mode of the radar.

2.2 Radar dodging and cognitive jamming

To conveniently evaluate the performance of CNR, the concept of radar dodging is proposed in this paper. Radar dodging refers to the behaviours of estimating and predicting jamming modes by detecting channel parameters, and then avoiding the jamming-covered fields. Correspondingly, we can define the concept of CNJ as follows: a set of jamming strategies used to maximise jamming rate for future time periods, which is generated by the successfully estimating and predicting for the radar dodges of target radar. The jamming rate (η) can be calculated using

$$\eta = \frac{T_{\text{jam}} - T_{\text{del}}}{T_{\text{radar}}}\%, \quad (1)$$

where T_{jam} is the time period of jamming release, T_{delay} is the processing delay of the jammer, and T_{radar} is the duration of the radar mission.

Fig. 1 is a good way to explain the process of improving the jamming rate of CNJ. As shown, if the CNR succeeds in getting rid of the jamming channel, the jamming rate will become low, whereas when the jammer predicts all radar dodges of the radar, the interference rate will be particularly high (close to 1).

Actually, the traditional jammers use intermittent sampling to obtain the radar parameters at different time intervals instead of CNJ, and the jamming rate is computed using

$$\eta = \rho \times \frac{T_{\text{jam}} - \sum_{i=1}^{n} T_{\text{int},i} - \sum_{i=1}^{N} T_{\text{del},i}}{T_{\text{radar}}}\%, \quad (2)$$

where $T_{\text{int},i}$ and $T_{\text{delay},i}$ are the identification time and processing delay of the jammer at the ith sample, respectively. n ($n \geq 1$) is the number of intermittent sampling pulses, and N ($N \geq 1$) is the number of radar pulses. ρ is the cognation rate of radar signals during sampling. It is assumed that the arrival time of the radar pulse and the sampling time of the jammer are not related in a certain time interval. It can be considered that the probability of the radar signal being successfully captured is uniformly distributed in the time interval, i.e. $\rho = n/N$.

For (2), improving the number of pulses of intermittent sampling can definitely improve the recognition performance for radar signals ($\rho \to 1$);

It is difficult to find a compromise scheme between the two due to the time delay and recognition time depending on the jamming technology and the physical performance of the jammer. The obvious result is that CNJ can greatly reduce the amount of intermittent sampling, but the cognation rate remains unchanged.

Additionally, the following two points need to be supplemented: (1) to better analyse the effects of CNJ, we suppose that the CNR only generates radar dodges for current jamming, but for the jammer, there is no limit to the prediction step size of CNJ; (2) in the real battlefield, the one-to-one jammer-radar process is not common. However, due to limited space, this paper does not discuss the high-complexity multiple-to-multiple jammer-radar process, although the method presented in this paper is still applicable to that scenario.

3 Jammer-radar game

Consider the encounters of the radar and the jammer as a card game. For the radar, each time the radar stage progresses, a card is played, and the better the card is, the higher the score. During this time, the jammer needs to continuously play deducting-point cards to make the score of the radar lower and lower.

3.1 Players and their cards

In the game, a CNR is regarded as a defence decision agent. It is assumed that the modes of the radar can be divided into four stages in the following order: search, acquisition, tracking, and guidance. There is a certain execution time in each radar stage. We set the execution time between these four stages to be 10, 5, and 10 PRIs, respectively. Additionally, if the performance of the radar drops to a performance threshold, the radar stage will reset to the search stage within a fixed period. This threshold can be a user-defined parameter, such as 0.6, representing that the performance threshold of resetting the radar is 60%.

Plus, the design parameters of the radar echo signal include: the initial CF is 6 G, and the adjustment interval is 2 to 10 G; the initial power is 10 W, and the adjustment interval is 10 to 50 W; the bandwidth (BW) is 50 M; the pulse width is 40 ns; and the PRI is 10 µs. The radar can continuously transmit a maximum of three different modulation signals/waveforms.

The other player, i.e. a cognitive jammer, is regarded as an attack decision agent. It is assumed that the jammer in the game is equipped with three jamming technologies: multiple false targets (MFT), noise jamming (NJ), and range-velocity simultaneous pull off (RVSPO). The design parameters of the jamming signal received by the radar include: the maximum CF is 10 G; the maximum BW is 100 M; the maximum power is 1 kW; the intermittent sampling time is 5 ns; and the processing delays of the above three jamming technologies are 10, 5, and 10 ns, respectively.

Table 1 Stage effectiveness factors

Stage	MFT	NJ	RVSPO
search	1.0	0.8	−1.0
acquisition	1.0	0.8	−1.0
tracking	0.0	−1.0	1.0
guidance	0.0	−1.0	1.0

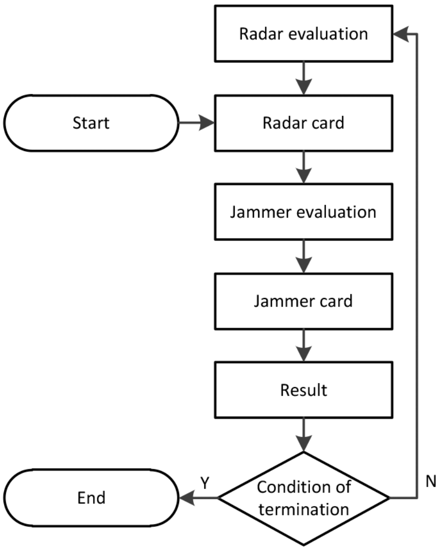

Fig. 2 *Flow chart of the jammer-radar game*

3.2 Game rules

Based on the setting parameters, we evaluate the interaction between different radar stages and jamming technologies, and then write rules for how the cards interact in the game.

3.2.1 Jammer card for NJ: Jamming factor (E) is an important index to describe the jamming performance of NJ (e.g. the jamming factor of 0.6 indicates a 60% drop in radar performance), which can be computed using

$$E = \mathrm{LUT}(S, Y) \times \eta \times [1 - exp(-T_{\mathrm{FB}}/T_0)]\,. \tag{3}$$

where T_{FB} is the coverage rate of interference temperature, and the calculation formula of T_{FB} is

$$T_{\mathrm{FB}} = \begin{cases} \dfrac{P_J \cap B}{P_R B_R} & \text{if } \cap B < B_R \\ \dfrac{P_J}{P_R} & \text{else} \end{cases}. \tag{4}$$

LUT is a user-defined look-up table shown in Table 1. $\mathrm{LUT}(S, Y)$ denotes the radar stage effectiveness, i.e. the effects of different jamming technologies (Y) on different radar stages (S) (a negative number indicates illumination of the platform) [11]. P_J and P_R are the mean signal powers of the jammer and radar entering the radar receiver, respectively. $\cap B$ is the overlap of the jamming signal and radar signal in the frequency domain, where the spectrum interval of the jamming signal is expressed as $[f_J - B_J/2, f_J + B_J/2] \pm \delta$. B_J is the jamming BW, f_J is the CF of the signal, and δ is estimation error. Similarly, the spectrum interval of the radar signal is $[f_R - B_R/2, f_R + B_R/2]$. T_0 is a constant related to radar sensitivity; we set it to 60.

For traditional jamming, the choice of CF is related to the estimated-level of intermittent sampling, whereas CNJ depends on the prediction effect. To compare the effects of above two jamming types, let the δ of traditional jamming be 0, while the δ of CNJ be 50 M.

For (3), the jamming factor can be considered as the combined benefits of a jammer based on the time, frequency, and energy, as well as the jamming strategy. Obviously, the requirement of NJ is that the maximum jamming power is maintained, while adjusting the BW of the jamming signal covering the BW of the radar signal.

3.2.2 Radar card for NJ: Spectrum shift is the countermeasure for NJ.

Adjust the waveform parameters and spectrum within 1 PRI. The method of waveform adjustment is to move the CF with the step size of 1 G and improve the transmit power to 50 W.

3.2.3 Jammer card for MFT: Equation (3) needs to be modified as follows when the jammer uses MFT:

$$E = \begin{cases} \mathrm{LUT}(S, Y) \times \eta & \text{if rand}\{1, 2, \ldots, M\} = M \\ 0 & \text{else} \end{cases}. \tag{5}$$

where M is the number of radar signal types. $\mathrm{rand}\{1, 2, \ldots, M\}$ is an integer randomly selected from 1 to M. As MFT will imitate all the characteristics of radar signal, the jamming will fail when the jammer is engaged by the wrong radar signal. The utilisation of MFT requires that the all of the parameters of the radar signal are within the boundary of the jamming parameters.

3.2.4 Radar card for MFT: Radio-frequency hiding is the countermeasure for MFT.

In the first PRI, after being jammed, three different modulating waveforms of the radar will be activated, including real echo.

3.2.5 Jammer card for RVSPO: For RVSPO, the process flow is divided into three phases when using uniform-gate pull off, and it can only produce effects for radar after N_1 PRIs, but the longer the time is, the easier the real echo of radar can be extracted. Hence, the jamming factor should be gradually attenuated. Equation (3) becomes

$$E = \begin{cases} 0 & \text{if } 0 \le n \le N_1 \\ \dfrac{\mathrm{LUT}(S, Y) \times \eta \times (n/N_2)}{\mu^{n - N_1}} & \text{if } N_1 \le n \le N_2 \\ \dfrac{\mathrm{LUT}(S, Y) \times \eta}{\mu^{n - N_1}} & \text{if } n > N_2 \end{cases}. \tag{6}$$

where n is the number of pulses that the radar is pulled, and $n = 1, 2, \ldots, N_2$. In this paper, we set the N_1, N_2 to 2, and 5, respectively; i.e. when the radar progresses to the N_2^{th} PRI, there is only a false echo in the radar's tracking wave, which makes the radar impossible to capture the true echo. μ is the echo separation index of the radar, and its initial value is 1. The greater the value, the better the radar's extraction performance for real echoes is. In addition, when the jamming factor is less than a user-defined value, it can be considered that the false target in the tracking-gate is completely separated. Therefore, it is necessary to change the waveform characteristic of RVSPO by resetting n.

3.2.6 Radar card for RVSPO: Pure waveform extraction is the countermeasure for RVSPO:

The pure data of the waveform is extracted from each PRI by the radar, which results in the jamming effect gradually weakening until target tracking is restored. When the radar progresses to the tracking stage, the transmit power and are adjusted to W and 1.1, respectively.

3.3 Conditions for the termination of the game

The winning condition of the defence decision agent is the CNR successfully entered the guidance task and continued for six PRIs. The winning condition of the attack decision agent is to complete a given mission and survive.

The flow chart of the game is given in Fig. 2.

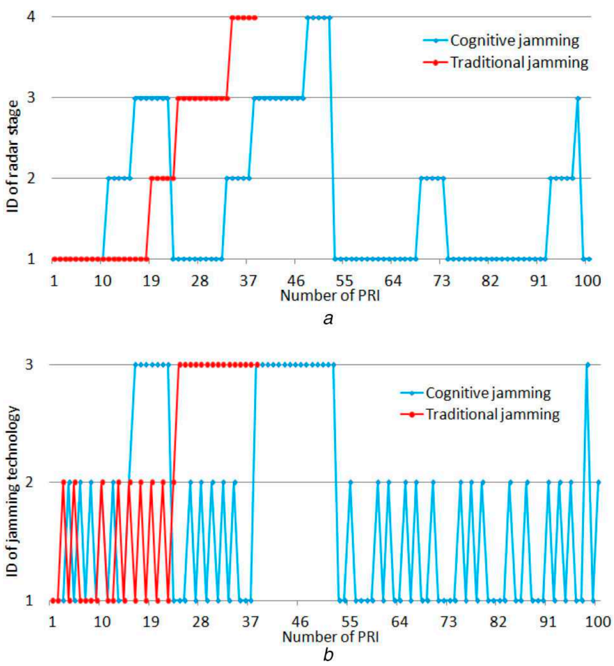

Fig. 3 *Continuous-time effects of cognitive jamming*
(a) Effects of different jammers on the jammer-radar game. The radar stage identity (ID) 1, 2, 3, 4 corresponds to the search, acquisition, tracking, and guidance stage in sequence, ***(b)*** Changes of jamming technologies of different jammers in the jammer-radar game. The jamming technology identity (ID) 1, 2, 3 corresponds to the MFT, NJ, RVSPO in sequence

4 Scenario simulation

The proposed game will be played in a more specific scenario.

In this scenario, the radar runs first, and then after a sampling pulse, the jammer engages with the radar, i.e. the game begins. Suppose the step size of signal prediction based on one intermittent sampling of CNJ is 1 PRI, while the traditional jamming does not predict. Set the reset threshold and the reset period of each radar stage to 0.5 and 3 PRIs, respectively. The total duration of the game is 1 ms. The reset threshold of RVSPO is set to 0.2. At the time of testing, the optimal game strategy of the other player is searched by an exhaustive method. Note that the objective function optimised for each player is the value of jamming factor (E^i_{best}) of the ith PRI, and the real jamming effect will be fed back to the jammer when the next PRI arrives. Therefore, the gain of the jammer in the whole game is the sum for all E^i_{best}.

Moreover, because of the randomness of prediction errors, we perform 50 independent Monte–Carlo tests in the simulation, and then compute the mean game progress (MGP) after 50 runs.

The mathematical model of the jammer-radar game, including related parameters, is simulated using MATLAB 2016a via a PC with i3 CPU with win7.

After simulation calculations, the MGPs of cognitive and traditional jamming were 98.3 and 31.8 (in PRI), respectively.

Since the total duration of the game is 100 PRIs, the survival rates of a cognitive and a traditional jammer are 98.3 and 31.8%, respectively. In comparison, the performance of the CNJ is more than twice that of traditional jamming, which is enough to reflect the superiority of the former.

By taking one game play of 50 runs as an example, we can better demonstrate the ability of CNJ. Figs. 3*a* and *b* show the specific game process and the corresponding jamming strategy for each PRI, respectively. It is seen that, the cognitive jammer wins, i.e. survives, in the game, but traditional jammer fails at the 38th PRI.

CNJ requires the identification and estimation of the radar's behaviours to achieve optimal jamming for the future. Since the state of the CNR is constantly changing to adapt to different electromagnetic spectrum environments, for traditional jamming, it is necessary to optimise the time of intermittent sampling to ensure the effectiveness of the jamming. From Figs. 3*a* and *b*, it can be seen that the MFT dominates the search and acquisition stage of the radar, but it will activate the radar state of radio-frequency hiding. Traditional jamming strongly depends on the effect of intermittent sampling, so MFT will fail when sampling the wrong data. However, CNJ predicts the transition of radar state. In the next step, the jammer discards the MFT's lower than expected return and chooses the NJ to keep the jamming factor at a certain level. In addition, after the radar enters the tracking stage, the RVSPO is the only choice for the cognitive and traditional jammer, but the cognitive jammer knows the feedback result of the radar one step ahead of time and selects a new set of jamming parameters to increase the jamming rate and jamming factor, which can reset the radar before it wins.

In brief, if the CNJ function accurately predicts the radar dodges, it can exert the full performance of the jamming strategy.

5 Conclusion

This paper establishes a radar countermeasure model for the jammer, namely, the jammer-radar game. First, the basic operational characteristics of CNR are concluded. It is considered that radar dodging is the key factor to improve the performance of radar. Second, according to the settings of the jamming strategy, an ordered process of the game (implying the realisation of CNJ) is designed, and the contents and rules of the game are analysed in detail. Finally, utilising the exhaustive method to search for the optimal jamming strategy during each time interval, through the results of 50 simulation tests, it can be seen that CNJ with one-step prediction capability is more likely to win the game. This reveals that the effective identification of radar dodges can greatly enhance the survival probability of jammer in the electronic warfare.

6 References

[1] Bachmann, D.J., Evans, R.J., Moran, B.: ‘Game theoretic analysis of adaptive radar jamming’, *IEEE Trans. Aerosp. Electron. Syst.*, 2011, **47**, (2), pp. 1081–1100

[2] Chen, C., Song, M., Xin, C.*, et al.*: ‘A game-theoretical anti-jamming scheme for cognitive radio networks’, *IEEE Netw.*, 2013, **27**, (3), pp. 22–27

[3] Zhu, Y., Jian, Y.: ‘A game-theoretic approach to anti-jamming in sensor networks’, *Inf. Sci.*, 2010, **78**, (3–4), pp. 161–187

[4] Mallik, R.K., Scholtz, R.A., Papavassilopoulos, G.P.: ‘Analysis of an on–off jamming situation as a dynamic game’, *IEEE Trans. Commun.*, 2002, **48**, (8), pp. 1360–1373

[5] Xu, J., Duan, L., Zhang, R.: ‘Proactive eavesdropping via cognitive jamming in fading channels’. IEEE Int. Conf. on Communications, Kuala Lumpur, Malaysia, 2016, pp. 2790–2806

[6] Osner, N.R., Plessis, W.P.D.: ‘Threat evaluation and jamming allocation’, *IET Radar Sonar Navig.*, 2017, **11**, (3), pp. 459–465

[7] Karasakal, O.: ‘Air defense missile-target allocation models for a naval task group’, *Comput. Oper. Res.*, 2008, **35**, (6), pp. 1759–1770

[8] Johansson, F., Falkman, G.: ‘Performance evaluation of TEWA systems for improved decision support’, *Lect. Notes Comput. Sci.*, 2009, **5861**, pp. 205–216

[9] Kang, S., Park, H., Noh, S., *et al.*: ‘Autonomously deciding countermeasures against threats in electronic warfare settings’. Int. Conf. on Complex, Intelligent and Software Intensive Systems, Fukuoka, Japan, 2009, pp. 177–184

[10] Chen, P., Wu, L.: ‘Waveform design for multiple extended targets in temporally correlated cognitive radar system’, *IET Radar Sonar Navig.*, 2016, **10**, (2), pp. 398–410

[11] Stinco, P., Greco, M.S., Gini, F.: ‘Spectrum sensing and sharing for cognitive radars’, *IET Radar Sonar Navig.*, 2016, **10**, (3), pp. 595–602